PREGÃO ELETRÔNICO N. 30/2025

LICITAÇÃO N. 1079455

O **SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL - SENAC,** Administração Regional em Santa Catarina, pessoa jurídica de direito privado, criado por Decreto Lei n. 8.621, de 10 de janeiro de 1946, com sua Administração Regional em Santa Catarina, inscrito no CNPJ sob o n. 03.603.739/0001-86, com sede na Rua Felipe Schmidt, 785, 6º e 7º andares, edifício Haroldo Soares Glavan, Centro, Florianópolis/SC, CEP 88010-002, por intermédio de sua Comissão Permanente de Licitação, constituída pela Portaria 18/2023, datada de 26 de dezembro de 2023, torna público, para ciência dos interessados, que por seu Pregoeiro, realizará licitação na Modalidade **PREGÃO ELETRÔNICO do tipo menor preço global do lote,** nos termos da Resolução Senac 1.270/2024, em vigor a partir de 2 de maio de 2024. As despesas decorrentes desta licitação correrão por conta de verbas específicas do Senac/SC, Centro de Custo: 900005003 - Padronização de Firewall Senac/SC, conforme requisições 234972 e 234965, e Processo n. 13073.

RESUMO DA LICITAÇÃO

OBJETO:
Aquisição de Firewalls e Softwares para ampliação, modernização e substituição de equipamentos.

RECEBIMENTO DA PROPOSTA ELETRÔNICA NO SISTEMA LICITAÇÕES-E2:
A partir das 15h do dia 22/10/2025 até às 11h do dia 30/10/2025

ABERTURA DAS PROPOSTAS ELETRÔNICAS NO SISTEMA LICITAÇÕES-E2:
A partir das 11h do dia 30/10/2025.

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS NO SISTEMA LICITAÇÕES-E2:
Às 11h do dia 30/10/2025.

DISPONIBILIDADE DO EDITAL:
No *site* https://licitacoes-e2.bb.com.br sob o número: **1079455** e no Site do **SENAC/SC** – https://licitacao.sc.senac.br/.

PEDIDOS DE ESCLARECIMENTO:
Impreterivelmente, até as 23h59 do terceiro dia útil anterior à data de abertura da sessão, pelo *e-mail* licitacao@sc.senac.br, em relação a eventuais dúvidas de interpretação do presente Edital e seus Anexos, visando à sua melhoria.

IMPUGNAÇÕES AO EDITAL:
Impreterivelmente, até as 23h59 do terceiro dia útil anterior à data de abertura da sessão, pelo *e-mail* licitacao@sc.senac.br, devendo ser enviada em papel timbrado da licitante e assinada pelo representante legal, cabendo ao Pregoeiro divulgar a decisão sobre a impugnação no prazo de até 2 (dois) dias úteis, contados de sua interposição.

PREGÃO ELETRÔNICO N. 30/2025

LICITAÇÃO N. 1079455

1. OBJETO

1.1. A presente licitação destina-se a Aquisição de FIREWALLS e Licenças Firewalls, de acordo com as condições, quantidade e exigências descritas neste Edital e seus anexos.

2. CONDIÇÕES GERAIS PARA PARTICIPAÇÃO

2.1. Respeitadas as condições legais e as constantes deste Edital, deverão ser observadas as seguintes determinações:

2.1.1. Na presente licitação somente poderá se manifestar em nome da licitante o sócio ou dirigente/administrador, com poderes conferidos pelo Estatuto ou Contrato Social em vigor, para representá-la ativa e passivamente em juízo ou fora dele, ou, ainda, procurador devidamente credenciado, ou seja, com poderes outorgados por meio de procuração, por instrumento público ou particular, para representar a licitante em processo licitatório.

2.2. NÃO PODERÃO PARTICIPAR DA PRESENTE LICITAÇÃO:

2.2.1. Empresas em processo de dissolução ou falência.

2.2.2. Empresas em que dirigentes ou empregados da entidade façam parte do quadro societário.

2.2.3. Pessoas físicas ou jurídicas que tenham sido punidas com suspensão do direito de contratar ou licitar com o **Senac/SC,** enquanto perdurarem os efeitos da penalidade aplicada.

2.2.4. Sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, desde que, em eventuais diligências, se comprove o conluio entre eles com intuito de frustrar a competitividade do certame, exceto se demonstrado que não agem representando interesse econômico em comum.

2.3. CREDENCIAMENTO:

2.3.1. Somente poderão participar deste Pregão Eletrônico as licitantes devidamente credenciadas no provedor do sistema "Licitações-e" no *site* https://licitacoes-e2.bb.com.br, por meio de atribuição de chaves de identificação e de senhas individuais, fornecidas pelo provedor do sistema, quando do credenciamento.

2.3.2. A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras as suas propostas e lances, sendo de sua inteira e exclusiva responsabilidade o uso da senha de acesso, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao **Senac/SC** responsabilidade por eventuais danos decorrentes de uso indevido de senha, ainda que por terceiros.

2.3.3. O credenciamento da empresa e de seu representante legal junto ao sistema eletrônico implica na responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

2.3.4. Os interessados obterão maiores informações sobre a apresentação de documentação e credenciamento de representantes em qualquer agência do Banco do Brasil S/A ou pelo telefone do suporte técnico 4004-0001 (capitais e regiões metropolitanas) ou 0800-729-0001 (demais localidade).

2.4. CONEXÃO COM O SISTEMA:

2.4.1. A participação neste Pregão Eletrônico se dará, exclusivamente por meio do sistema eletrônico, utilizando-se do *login* e senha da licitante e subsequente encaminhamento da proposta de preços, observadas as datas e os horários limites estabelecidos neste Edital.

2.4.2. A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras as suas propostas e lances.

2.4.3. Caberá à licitante acompanhar as operações no sistema eletrônico durante a Sessão Pública do Pregão Eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

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

2.4.4.1. O Pregoeiro, quando possível, dará continuidade à sua atuação no certame, sem prejuízo dos atos realizados.

2.4.4.2. Quando a desconexão persistir por tempo superior a 30 (trinta) minutos, a Sessão Pública do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa às licitantes, por meio do *site* https://licitacoes-e2.bb.com.br, no campo "opções > listar documentos".

3. PROPOSTA DE PREÇOS

3.1. Para fins de julgamento, será considerada a proposta em 2 (duas) formas não excludentes:

3.1.1. PROPOSTA ELETRÔNICA: Proposta de valor total por lote que deve ser enviada pela licitante, exclusivamente, por meio do sistema "licitações-e2", no *site* https://licitacoes-e2.bb.com.br, até às **11 (Onze) horas do dia 30/10/2025.**

3.1.1.1. Em nenhuma hipótese será admitida a identificação da licitante, sob pena de desclassificação.

3.1.1.2. O valor inserido no sistema sempre será pelo valor total do lote, considerando todos os itens descritos.

3.1.1.3. Caso a licitante deixe de apresentar valor para algum item, será desclassificada "em relação ao lote ao qual o item pertence (quando houver mais de um lote com vários itens)".

3.1.1.4. O valor total do lote englobará todas as despesas/custos diretos e indiretos, relativos à execução do objeto deste Edital, de acordo com as especificações técnicas contidas no **Anexo I – Termo de Referência** deste Edital.

3.1.1.5. No caso de empate entre 2 (duas) ou mais propostas, e não havendo lances, o desempate se fará, obrigatoriamente, por meio de sorteio, para o qual serão convocadas as licitantes.

3.1.1.6. Nenhuma documentação precisará ser inserida no sistema eletrônico. Devendo ser observado, para entrega da documentação, o constante do item 5.4 deste edital.

3.1.2 PROPOSTA AJUSTADA: Proposta detalhada enviada pela licitante arrematante, apresentada em papel timbrado com identificação da licitante, sem emendas, rasuras, assinada na última página e rubricada nas demais pelo representante legal da licitante.

3.1.2.1. Deverá apresentar prazo de validade da proposta, valor unitário e valor total arrematado.

3.1.2.2. Havendo divergência entre o preço unitário e total da proposta ajustada, prevalecerá o valor total arrematado e, havendo discordância entre o valor total da proposta em algarismo e o total por extenso, prevalecerá o que equivale ao valor arrematado.

3.1.2.3. Deverá conter o prazo de entrega conforme descrito no **Anexo III – Modelo e Proposta**.

3.1.2.4. A validade da proposta não poderá ser inferior a 60 (sessenta) dias a contar da data de abertura do Pregão Eletrônico (SUBITEM 5.2.1), cujos preços deverão ser fixos e irreajustáveis. Não sendo indicado o prazo de validade, fica subentendido como de 60 (sessenta) dias.

3.1.2.5. Caso haja o vencimento da validade da proposta sem que a licitação tenha sido homologada e adjudicada, esta ficará automaticamente prorrogada, exceto se houver manifestação contrária formal da licitante, pelo *e-mail* licitacao@sc.senac.br, dirigida à Comissão Permanente de Licitação, caracterizando seu declínio em continuar na licitação.

3.1.2.6. Os termos constantes da proposta de preços da arrematante são de exclusiva responsabilidade da licitante, não lhe assistindo o direito a qualquer modificação, após seu envio, sem a prévia concordância ou solicitação pela Comissão Permanente de Licitação.

4. HABILITAÇÃO

4.1. HABILITAÇÃO JURÍDICA:

4.1.1. Ato constitutivo, estatuto ou contrato social em vigor, acompanhado da última alteração contratual; ou

4.1.2. Última alteração contratual consolidada; ou

4.1.3. Inscrição do ato constitutivo em Cartório de Registro de Pessoas Jurídicas, no caso de sociedades simples não empresariais, acompanhada da prova da diretoria em exercício; ou

4.1.4. Registro comercial, em caso de empresa individual, Certificado da Condição de Microempreendedor Individual (CCMEI).

4.1.5. Ato de nomeação ou de eleição dos administradores, na hipótese de terem sido nomeados ou eleitos em separados.

4.1.6. Documento comprobatório do representante legal da licitante, por meio da apresentação de cópia de documento oficial de identidade com foto e CPF.

4.1.7. Estando a licitante em processo de recuperação judicial ou extrajudicial, certidão emitida pela instância judicial ou extrajudicial competente, ou documento similar, que certifique que a licitante está apta econômica e financeiramente a participar de procedimento licitatório.

4.1.8. A licitante arrematante deverá encaminhar os documentos referentes aos SUBITENS 4.1.1 a 4.1.5 devidamente registrados no órgão competente.

4.2. QUALIFICAÇÃO TÉCNICA:

4.2.1. Comprovar, através de documento(s) específico(s) (atestado de capacidade técnica), que comprove(m) ter a licitante executado, a contento, objeto similar ao descrito no **Anexo I – Termo de Referência**, a pelo menos 01 (um) órgão público ou empresa privada.

4.2.1.1. O documento deverá ser elaborado em papel timbrado da empresa privada ou órgão público e conter o nome legível, endereço e telefone do emitente.

4.2.2. Declaração de aceitação do edital, em papel timbrado da licitante, declarando ter tomado conhecimento e examinado, cuidadosamente, os documentos desta Licitação e de ter integralmente compreendido e aceito as condições estabelecidas para a contratação do objeto desta Licitação, conforme modelo de Proposta **Anexo III** deste Edital.

4.3. REGULARIDADE FISCAL:

4.3.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ).

4.3.2. Prova de regularidade perante a Fazenda Federal (Certidão Negativa de Débitos ou Positiva com Efeitos de Negativa Relativos aos Tributos Federais e à Dívida Ativa da União), a qual abrange, inclusive, as contribuições sociais previstas na Lei n.8.212/1991.

4.3.3. Prova de regularidade perante a Fazenda Estadual, do domicílio ou sede da Licitante, referente ao ICMS – Imposto sobre a Circulação de Mercadorias e Serviços. Em caso contrário deverá apresentar declaração informando não ser contribuinte.

4.3.4. Prova de regularidade perante a Fazenda Municipal, do domicílio ou sede da Licitante, referente ao ISS – Imposto sobre Serviços. Em caso contrário deverá apresentar declaração informando não ser contribuinte.

4.3.5. Certificado de Regularidade de Situação (CRF), comprovando situação regular perante o Fundo de Garantia do Tempo de Serviço (FGTS).

4.4. CONSIDERAÇÕES GERAIS SOBRE OS DOCUMENTOS:

4.4.1. Os documentos que forem emitidos pela internet estarão sujeitos a posterior conferência na página eletrônica do órgão emissor.

4.4.2. O pregoeiro poderá realizar diligências para a complementação de informações necessárias à apuração de fatos existentes à época da abertura do certame, bem como poderá admitir a juntada de documentos pelas licitantes que apenas venham a atestar condição pré-existente à abertura da sessão pública do certame.

4.4.3. Os documentos deverão ser apresentados em fotocópias legíveis e dentro dos respectivos prazos de validade, não sendo aceitos quaisquer tipos de protocolos ou guias de pagamento. Quando qualquer um dos documentos não mencionar a data de validade, considerar-se-ão com validade de 90 (noventa) dias, a contar da data da emissão, salvo os documentos utilizados como comprovação de inscrição cuja autenticidade possa ser verificada por meio de consulta em sítios eletrônicos.

4.4.4. Em se tratando de filial, esta fica desobrigada de apresentar os documentos dos SUBITENS 4.1 e 4.3.3, desde que tenham sido apresentados pela matriz. Os demais documentos deverão ser apresentados, pela matriz e filial, separadamente, emitidos com os respectivos CNPJs.

4.4.5. Independentemente de declaração expressa, a apresentação dos documentos de habilitação e da proposta ajustada implica a aceitação plena e total das condições e exigências deste Edital e seus **Anexos**, a veracidade e autenticidade das informações constantes na proposta ajustada e nos documentos de habilitação apresentados, e ainda, a inexistência de fato impeditivo à participação da licitante, o qual, na incidência, obriga a licitante a comunicar ao **Senac/SC** quando ocorrido durante o certame.

4.4.6. Os documentos redigidos em língua estrangeira deverão ser traduzidos para a língua portuguesa, e vir acompanhados de tradução juramentada.

4.4.7. A habilitação da licitante estrangeira poderá ser comprovada por meio da apresentação de seus atos constitutivos ou documentos similares e de documentos de habilitação técnica, dispensada a apresentação da comprovação das habilitações fiscal e econômico-financeira.

4.4.8. O desatendimento de exigências meramente formais que não comprometam a aferição da qualificação do licitante ou a compreensão do conteúdo de sua proposta não importará seu afastamento da licitação ou a invalidação do processo.

4.4.9. É permitida a inclusão de documento complementar ou atualizado, desde que não alterem a substância das propostas, dos documentos e sua validade jurídica e seja comprobatório de condição atendida pelo licitante quando apresentada sua proposta, que não foi juntado com os demais documentos por equívoco ou falha, o qual deverá ser solicitado e avaliado pela comissão de licitação/pregoeiro/leiloeiro.

4.4.10. Não serão levados em consideração os documentos e/ou propostas que não estiverem de acordo com as condições deste Edital e seus **Anexos**, quer por omissão, quer por discordância.

5. PROCEDIMENTOS LICITATÓRIOS

5.1. RECEBIMENTO DAS PROPOSTAS ELETRÔNICAS:

5.1.1. Até às **11 (onze) horas do dia 30/10/2025**, os interessados poderão inserir ou substituir propostas de preços no sistema eletrônico.

5.2. ABERTURA DAS PROPOSTAS ELETRÔNICAS:

5.2.1. Às **11 (onze) horas do dia 30/10/2025,** procederemos a abertura das propostas de preços no sistema eletrônico.

5.2.2. A apresentação da proposta eletrônica pressupõe o fiel cumprimento do estabelecido neste Edital e seus **Anexos**, inferindo-se, portanto, a não necessidade de análise para fins de classificação de propostas. Não obstante ao disposto neste SUBITEM, o Pregoeiro, a seu exclusivo critério, poderá optar por realizar a referida análise e desclassificar as propostas que não estejam de acordo com o estabelecido neste Edital e seus **Anexos**, cabendo ao Pregoeiro registrar e disponibilizar a decisão no sistema eletrônico para acompanhamento em tempo real pelas licitantes.

5.2.2.1. Caso o Pregoeiro opte por realizar análise de propostas, da decisão de desclassificação somente caberá pedido de reconsideração ao Pregoeiro, a ser enviado exclusivamente pelo *e-mail* licitacao@sc.senac.br, acompanhado da justificativa e suas razões, no prazo de 30 (trinta) minutos a contar do momento em que vier a ser disponibilizada no sistema eletrônico a decisão a ser impugnada.

5.2.2.2. O Pregoeiro decidirá no mesmo prazo, salvo motivos que justifiquem a sua prorrogação, cabendo ao Pregoeiro registrar e disponibilizar a decisão no sistema eletrônico para acompanhamento em tempo real das licitantes.

5.2.2.3. Havendo necessidade, o Pregoeiro poderá suspender a sessão.

5.2.2.4. Da decisão do Pregoeiro relativa ao pedido de reconsideração não caberá recurso.

5.2.3. Serão, ainda, desclassificadas as propostas que sejam omissas, vagas, com valores simbólicos, irrisórios, de valor zero ou que apresentem irregularidades capazes de dificultar o julgamento.

5.3. SESSÃO PÚBLICA DE LANCES:

5.3.1.A disputa de lances ocorrerá em modo aberto, conjuntamente, com critério de julgamento menor preço, e terá início às **11 (onze) horas do dia 30/10/2025**. As licitantes classificadas poderão oferecer lances exclusivamente pelo sistema eletrônico, sem restrições de quantidades de lances ou de qualquer ordem classificatória ou cronológica específica, mas sempre inferior ao seu último lance ofertado.

5.3.2. Não serão aceitos 2 (dois) ou mais lances do mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar pelo sistema eletrônico.

5.3.3. A licitante poderá oferecer lances sucessivos, observando o horário fixado e as regras de aceitação dos lances.

5.3.4. Aberta a sessão de disputa, que ocorrerá por limitados 15 (dez) minutos, sem prorrogações, onde nesta fase as empresas licitantes poderão oferecer lances sucessivos, não sendo aceitos 2 (dois) ou mais lances do mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar pelo sistema eletrônico.

5.3.5. Após o tempo estipulado no item 5.3.4, inicia-se o período aleatório, ainda em modo aberto de disputa, onde o tempo de duração desta fase será de até 10 (dez) minutos, com fechamento iminente dos lances, iniciando, na sequência, o modo de disputa fechada.

5.3.6. Encerrado o modo aberto de disputa, os autores das ofertas com valores até 10% (dez por cento) superiores à oferta mais vantajosa, serão convocados pelo sistema para que ofertem um lance final e fechado em até 5 (cinco) minutos da convocação.

5.3.7. Não havendo no mínimo 3 (três) ofertas, nas condições citadas no item 5.3.6, o sistema convocará os autores dos melhores valores subsequentes, no máximo de 3 (três), para ofertarem lance final e fechado.

5.3.8. O(s) licitante(s) poderá(ão) optar por manter o seu último lance da etapa aberta, ou por ofertar valor menor, em até 5 (cinco) minutos após a convocação.

5.3.9. O 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, será de **R$ 100,00 (cem reais)**.

5.3.10. Encerrado o modo fechado de disputa, o sistema ordenará todos os valores que foram convocados para a etapa fechada, em ordem de vantajosidade, onde a proposta inicial também será considerada como o primeiro lance da disputa, e o licitante poderá optar por manter, na etapa fechada, o seu lance final da etapa aberta.

5.3.11. Quando houver somente propostas iniciais sem lances, serão aplicados os critérios de desempate, por meio de sorteio, para o qual serão convocadas as licitantes. previsto no item 3.1.1.5 do instrumento convocatório.

5.3.12. Durante a sessão no modo aberto de disputa, as licitantes serão informadas, em tempo real, sobre o valor do menor lance registrado, sem identificação da licitante.

5.3.13. Se alguma licitante fizer um lance que esteja em desacordo com o Edital, ou oferta inexequível, este poderá ser cancelado pelo Pregoeiro, por meio do sistema eletrônico. Será emitido na tela um aviso e na sequência o Pregoeiro justificará o motivo da exclusão por meio de mensagem às licitantes.

5.3.14. O sistema informará a proposta de menor preço imediatamente após o encerramento da sessão. As licitantes deverão consultar regularmente o sistema eletrônico para verificar o resultado da licitação.

5.3.15. Após o encerramento do modo fechado, antes de ser declarada vencedora, o Pregoeiro encaminhará, pelo sistema eletrônico, contraproposta diretamente à licitante que tenha apresentado o lance de menor preço para o lote.

5.3.16. A negociação será realizada por meio do sistema eletrônico, podendo ser acompanhada pelas demais licitantes.

5.3.17. O sistema eletrônico gerará ata circunstanciada da sessão, na qual estarão registradas a indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas a sessão e os autores dos lances

5.4. ENVIO DOS DOCUMENTOS DE HABILITAÇÃO E PROPOSTA DE PREÇOS AJUSTADA:

5.4.1. Ordenados os lances em forma crescente de preço, o Pregoeiro determinará a licitante classificada em primeiro lugar, denominada ARREMATANTE, que encaminhe, até às 18h do dia útil subsequente, a contar do término da referida sessão, os documentos de habilitação descritos no

ITEM 4 deste Edital, e a PROPOSTA AJUSTADA, conforme previsto no SUBITEM 3.1.2 deste Edital.

5.4.4.1. Os documentos citados no SUBITEM acima deverão ser encaminhados, exclusivamente, pelo *e-mail* licitacao@sc.senac.br, indicando no campo ASSUNTO o número da licitação.

5.4.2. A proposta de preço ajustada e a documentação de habilitação poderão ser solicitadas em original ou por cópia autenticada a qualquer momento, no prazo a ser estabelecido pelo Pregoeiro, caso em que deverão ser entregues, obrigatoriamente, em envelope único lacrado, no qual, externamente, deverá ser informado o nome da licitante, o número da presente licitação e a inscrição "proposta de preços e documento de habilitação" na Rua Felipe Schmidt, 785, 7° andar, edifício Haroldo Soares Glavan, Centro, Florianópolis/SC, CEP 88010-002, Setor de Licitações.

5.4.3. A não apresentação da proposta de preço ajustada e da documentação completa de habilitação exigidos ou da apresentação de algum documento vencido, dentro do prazo e nas condições descritas no SUBITEM 5.4.1, observado o disposto no SUBITEM 4.4.2, poderá ocasionar a desclassificação da licitante, sendo convocadas, por ordem de classificação, as demais participantes do processo licitatório. Se for necessário, repetirá esse procedimento, sucessivamente, até a apuração de uma oferta que atenda ao Edital.

5.4.4. Na hipótese de inabilitação de todos os licitantes ou de desclassificação de todas as propostas, será dado o prazo de até 5 (cinco) dias úteis contados do dia seguinte ao comunicado, para apresentação de documentação de habilitação ou de propostas retificadas.

5.4.5. Com relação a proposta ajustada, mesmo tendo sido realizada análise e classificação da proposta eletrônica, conforme previsto no SUBITEM 5.2.2 deste Edital, caso seja identificada divergência com o previsto neste Edital e seus **Anexos**, o Pregoeiro poderá desclassificar a proposta ajustada.

5.5. DECLARAÇÃO DA LICITANTE VENCEDORA:

5.5.1. Realizada a análise nos documentos de habilitação e da proposta ajustada, o Pregoeiro indicará a licitante vencedora, consignando esta decisão e os eventos ocorridos em ata, que será disponibilizada pelo sistema eletrônico. O processo será encaminhado à autoridade competente para homologação e adjudicação.

5.5.2. A validade desta licitação não ficará comprometida por ter uma única licitante e/ou uma única proposta, sendo necessário, para ter validade, a justificativa da Comissão Permanente de Licitação ratificada pela autoridade competente.

5.5.3. Da decisão que declarar a licitante vencedora caberá recurso, fundamentado e dirigido à Comissão Permanente de Licitação. O recurso deverá ser encaminhado para o e-mail licitacao@sc.senac.br, no prazo de até 2(dois) dias úteis, a contar da data da divulgação da decisão, no sistema eletrônico. O recurso interposto tempestivamente terá efeito suspensivo.

5.5.4. A licitante que puder vir a ter a sua situação efetivamente prejudicada em razão de recurso interposto poderá sobre ele se manifestar no mesmo prazo de até 2 (dois) dias úteis, contados da sua ciência

5.5.5. Os recursos serão julgados pela Comissão Permanente de Licitação, no prazo de até 10 (dez) dias úteis, contados da data final para sua interposição.

5.5.6. As interessadas poderão solicitar vista dos autos do processo licitatório pelo *e-mail* licitacao@sc.senac.br. O processo poderá ser consultado fisicamente no endereço descrito no preâmbulo do Edital, pelo período de 5 (cinco) dias úteis contados da divulgação.

5.6. FORMALIZAÇÃO DO CONTRATO:

5.6.1. Homologado o resultado da licitação pela autoridade competente, o **Senac/SC** comunicará a licitante vencedora para formalizar o contrato no prazo de até 10 (dez) dias úteis a contar do recebimento do comunicado.

5.6.2. O prazo de convocação poderá ser prorrogado 1 (uma) vez, mediante solicitação da parte durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pelo **Senac/SC**.

5.6.3. Decorrido o prazo de validade da proposta sem convocação para a contratação, ficarão os proponentes selecionados liberados dos compromissos assumidos.

5.6.3.1. As condições, prazos, obrigações e demais disposições contratuais para a correta execução do objeto desta licitação estão estabelecidas no **Anexo IV** – Minuta de Contrato deste Edital de Pregão Eletrônico n. 30/2025.

6. SANÇÕES APLICÁVEIS NO PROCEDIMENTO LICITATÓRIO:

6.1. A licitante vencedora que, injustificadamente, não mantiver a proposta de preços durante o período da validade, recusar-se a assinar o contrato ou retirar o instrumento equivalente, no prazo estipulado no subitem 5.6.1 deste Edital, sujeitar-se-á aplicação das sanções de perda do direito à contratação, perda da caução em dinheiro ou execução das demais garantias de propostas oferecidas e de suspensão do direito de licitar e contratar com o **Senac/SC**, pelo período de até 3 (três) anos, conforme artigo 39 da Resolução Senac 1.270/2024.

6.2. A licitante perderá o direito de licitar, com abrangência nacional, com o **Senac/SC**, nos termos do artigo 41 da Resolução Senac 1.270/2024, nas seguintes hipóteses:

6.2.1. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato.

6.2.2. Fraudar a licitação ou praticar ato fraudulento na execução do contrato.

6.2.3. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.

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

6.3. Antes da aplicação de qualquer penalidade será facultada à parte contrária a defesa, mediante envio de notificação escrita à licitante vencedora, a qual deverá ser respondida no prazo de até 5 (cinco) dias úteis ou outro a ser fixado pelo **Senac/SC.**

6.4. O descumprimento total ou parcial das condições, prazos e obrigações contratuais, relacionadas à execução do objeto, poderá ensejar a aplicação das sanções previstas no **Anexo IV** – Minuta de Contrato, sem prejuízo da responsabilização civil e penal, garantindo-se em qualquer hipótese o direito ao contraditório e à ampla defesa.

7. PROTEÇÃO DE DADOS PESSOAIS

7.1. As partes obrigam-se a atuar na contratação oriunda deste Edital em conformidade com a legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial a Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

7.2. Na execução do objeto deste Edital, nos termos do art. 5º, inciso VI e VII, da Lei n. 13.709/2018, o **Senac/SC** será o controlador e a licitante vencedora será a operadora dos dados pessoais. As obrigações e responsabilidades de cada uma das partes no tratamento de dados pessoais observarão as disposições previstas na legislação aplicável, além das Cláusulas constantes do Contrato.

7.3. Fica estipulado que as Partes deverão se adequar em caso de modificação dos textos legais indicados no SUBITEM acima ou de qualquer outro, de forma que exija modificações na estrutura do escopo do Contrato ou na execução das atividades ligadas a eles.

7.4. Se houver alguma disposição que impeça a continuidade da contratação do objeto deste certame conforme as disposições acordadas, o **Senac/SC** poderá resolvê-la sem qualquer multa, penalidade, ou indenização, apurando-se os serviços prestados e/ou produtos fornecidos até a data da rescisão e consequentemente valores devidos correspondentes.

7.5. A licitante vencedora deve dar ciência aos seus empregados, diretores, prepostos, clientes, fornecedores e parceiros sobre as legislações vigentes sobre Proteção de Dados Pessoais e garantir que possui todos os consentimentos e avisos necessários para permitir o tratamento de dados pessoais dos respectivos titulares a serem necessários para a execução do serviço.

7.6. A licitante vencedora, neste ato, garante ao **Senac/SC** que todos os dados pessoais coletados, produzidos, receptados, classificados, utilizados, acessados, reproduzidos, transmitidos, distribuídos, processados, arquivados, armazenados, eliminados, avaliados ou controlados pela informação, modificados, comunicados, transferidos, difundidos ou extraídos em razão do Contrato, serão tratados em conformidade com as legislações vigentes aplicáveis, sob pena de indenizar ao **Senac/SC** pelos prejuízos que este venha a incorrer em razão de eventuais demandas judiciais ou administrativas, que sejam prejuízos, moral, material ou perdas e danos ocasionados ao **Senac/SC**, seus empregados, clientes ou fornecedores e parceiros, tais como, mas não se limitando a, despesas como honorários advocatícios, custas judiciais e taxas administrativas.

7.7. A licitante vencedora se obriga a realizar a correção, eliminação, anonimização ou bloqueio de dados, quando notificada pelo **Senac/SC**, nos casos de requisição do titular de dados pessoais ao **Senac/SC**.

7.8. A licitante vencedora deverá manter registro das operações de tratamento de dados pessoais que realizar, bem como deverá adotar as melhores práticas e implementar medidas técnicas e organizativas necessárias para proteger os dados contra situações, acidentais ou ilícitas, de destruição, perda, alteração, comunicação, difusão, acesso não autorizado, ou qualquer outra forma de tratamento inadequado ou ilícito, além de garantir a segurança no âmbito do tratamento de dados pessoais.

7.9. A licitante vencedora deverá notificar ao **Senac/SC**, imediatamente, por *e-mail* aos fiscais indicados neste Edital, em caso de reclamações e solicitações que venha a receber do titular de dados pessoais, bem como notificações, citações ou intimações judiciais ou administrativas em relação à conformidade com a proteção de dados identificadas em razão da contratação objeto deste Edital.

7.10. A licitante vencedora deverá notificar ao **Senac/SC**, por *e-mail* aos Fiscais indicados neste Edital, em 24h (vinte e quatro horas), em virtude de:

7.10.1. Qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de dados pessoais;

7.10.2. Qualquer descumprimento das obrigações contratuais relativas ao processamento e tratamento dos dados pessoais; e

7.10.3. Qualquer violação de segurança no âmbito das atividades da licitante vencedora.

7.11. As partes comprometem-se a cooperar entre si, auxiliando, na medida do razoável, no cumprimento de obrigações judiciais ou administrativas, de acordo com a Lei Geral de Proteção de Dados Pessoais aplicável, fornecendo as informações disponíveis e ações necessárias para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança, com relação aos dados pessoais utilizados na execução do objeto do presente Edital.

7.12. O disposto no item acima, ou eventual descumprimento de quaisquer deveres ou obrigações legais, contratuais, judiciais ou administrativos por uma das partes contratantes, não gera responsabilidade solidária ou subsidiária da outra parte, ficando somente a parte responsável, nos termos da lei, sujeita às sanções legais e contratuais pertinentes.

7.13. O **Senac/SC** terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da licitante vencedora com a Proteção de Dados Pessoais, sem que implique em qualquer diminuição da responsabilidade da licitante vencedora.

7.14. A contratação decorrente do objeto deste certame não transfere a propriedade de quaisquer dados do **Senac/SC** ou dos seus empregados, clientes, fornecedores e parceiros para a licitante vencedora.

7.15. A licitante vencedora se obriga a não utilizar, compartilhar ou comercializar quaisquer dados pessoais, que se originem e sejam criados a partir do tratamento de dados pessoais, que tenha acesso em razão de contratação oriunda deste certame.

7.16. Cada parte obriga-se a manter o mais absoluto dever de sigilo e confidencialidade relativamente a toda e quaisquer informações e dados pessoais tratados a que ela ou quaisquer de seus diretores, empregados e/ou prepostos venham a ter acesso, conhecimento ou que venha a lhe ser confiado em razão da celebração e execução do objeto deste certame.

8. DISPOSIÇÕES GERAIS

8.1. As decisões relativas a esta licitação, assim como eventuais alterações no Edital e seus **Anexos**, serão comunicadas pelo *site* https://licitacoes-e2.bb.com.br, no campo "opções > listar documentos", e, no Site do SENAC/SC – licitacao.sc.senac.br, https://licitacao.sc.senac.br/, opção de Link: Serviços/Área do Fornecedor/Licitações.

8.2. Todas as referências a horário neste Edital consideram o horário de Brasília-DF.

8.3. Na contagem dos prazos estabelecidos no presente Edital, excluir-se-á o dia do início e incluir-se-á o dia do vencimento, e considerar-se-á os dias consecutivos, exceto quanto for explicitamente disposta em contrário. Só se iniciam e vencem os prazos aqui referidos em dia de funcionamento do **Senac/SC.**

8.4. É facultada à Comissão Permanente de Licitação, em qualquer fase da licitação, a promoção de diligências destinadas a esclarecer ou complementar a instrução do processo licitatório, sendo admitida a juntada de documentos pelas licitantes que apenas venham a atestar condição pré-existente à abertura da sessão pública do certame.

8.4.1. A Comissão Permanente de Licitação tem o direito de exigir, a qualquer época ou oportunidade, documentos ou informações complementares que julgar necessários ao entendimento e comprovação dos documentos apresentados.

8.5. A Comissão Permanente de Licitação poderá efetuar visita às instalações da licitante classificada em primeiro lugar para confirmar as reais condições para atendimento do objeto desta licitação. Caso seja verificada a incapacidade do atendimento, a licitante poderá ser desclassificada, a critério da Comissão de Licitação.

8.6. A Comissão de Licitação poderá, no interesse do **Senac/SC** em manter o caráter competitivo desta licitação, relevar omissões puramente formais nos documentos e propostas apresentadas pela licitante. Poderá, também, realizar pesquisa na internet, quando possível para verificar a regularidade/validade de documentos ou fixar prazo às licitantes para dirimir eventuais dúvidas. O resultado de tais procedimentos será determinante para fins de habilitação.

8.7. Não serão levados em consideração os documentos e proposta que não estiverem de acordo com as condições deste Edital e seus **Anexos**, quer por omissão, quer por discordância.

8.8. Admitir-se-á a continuidade do Contrato celebrado com a licitante vencedora que tenha sofrido operações de reorganização societária, tais como cessão ou transferência total ou parcial, transformação, fusão, cisão e incorporação, desde que sejam observados pela nova empresa os requisitos de habilitação previstos neste instrumento convocatório e em conformidade com a Resolução Senac n. 1.270/2024, e ainda, que sejam mantidas as condições inicialmente estabelecidas.

8.9. Considerando que os procedimentos licitatórios não têm natureza jurídica de propostas de contratação, o **Senac/SC** reserva o direito de adiar, cancelar, revogar, anular ou tornar sem efeito, no todo ou em parte, a presente licitação sem que isto gere aos licitantes qualquer direito, inclusive de reparação a eventuais perdas e danos ou de lucros cessantes.

8.10. A inobservância ao Regulamento de Licitações e Contratos do Senac (Resolução Senac n. 1.270/2024) pode ensejar, em caso de comprovado prejuízo ao patrimônio do **Senac/SC**, a anulação da contratação resultante do procedimento irregular e a adoção de providências para responsabilização civil e penal dos que tenham contribuído com ação ou omissão para o resultado danoso.

8.11. Os prepostos da licitante vencedora não terão vínculos empregatícios e previdenciários de qualquer natureza com o **Senac/SC**.

8.12. A licitante vencedora e seus sucessores se responsabilizarão por todos e quaisquer danos e/ou prejuízos que, a qualquer título, venham causar à imagem do **Senac/SC** e/ou terceiros, em decorrência da execução indevida do objeto desta licitação.

8.13. A licitante declara ter ciência e se compromete a cumprir os princípios e regras contidos no Código de Ética do **Senac/SC**, disposto no site: https://transparencia.senac.br/#/sc/controle-interno-externo

8.14. A licitante declara ter ciência e se compromete a cumprir os princípios e regras contidos nas diretrizes com relação ao Programa de Integridade disposto no site: https://portal.sc.senac.br/doc/area-do-fornecedor/politica-de-conduta-fornecedores-servicos-senac.pdf

8.15. Considerando as medidas de segurança e boas práticas adotadas pelo **Senac/SC**, será de responsabilidade da licitante a confirmação do recebimento dos e-mails enviados para o endereço eletrônico licitacao@sc.senac.br. O **Senac/SC** não se responsabilizará por e-mails não recebidos e não confirmados pela licitante, independente do motivo que o ensejou.

8.16. Fica eleito o Foro da Comarca de Florianópolis/SC, com exclusão de qualquer outro, por mais privilegiado que seja, para dirimir quaisquer questões relativas referentes ao presente Edital.

8.16. Faz parte integrante deste Edital, os seguintes **Anexos**:

8.16.1. **Anexo I** – Termo de Referência.

8.16.2. **Anexo II** – Aceitação das Condições do Edital.

8.16.3. **Anexo III** – Modelo de Proposta.

8.16.4. **Anexo IV** - Minuta de Contrato.

Florianópolis, 22 de Outubro de 2025.

Comissão Permanente de Licitação

PREGÃO ELETRÔNICO N. 30/2025

LICITAÇÃO N. 1079455

ANEXO I –TERMO DE REFERÊNCIA

1. DO OBJETO

- Aquisição de novos firewalls e softwares para ampliação, modernização e substituição de equipamentos, conforme condições e especificações técnicas descritas neste documento.

2. DA JUSTIFICATIVA PARA CONTRATAÇÃO

- Como acontece com maioria das tecnologias, os ativos de rede sofrem um processo de depreciação natural que, associado ao avanço das tecnologias, imprime aos gestores a tomada de medidas que garantam a continuidade dos serviços de forma eficaz para a continuidade dos serviços.

- Devido ao aumento da demanda por conexões mais rápidas e estáveis faz-se necessária a aquisição e instalação de mais equipamentos para atendimento destas novas solicitações, além da substituição de ativos menos performáticos.

3. DA JUSTIFICATIVA PARA PADRONIZAÇÃO

- Com intuito de garantir o melhor desempenho, disponibilidade e estabilidade, sabendo que todas as unidades utilizam os mesmos equipamentos e administrados de maneira centralizada, faz-se necessário o uso de políticas, protocolos e tecnologias que visam principalmente garantir a segurança das informações e o melhor desempenho dos serviços e aplicações, e por isso adotaremos a prática de padronização do parque.

- Além das razões acima, justifica-se a manutenção da marca:

    - **Investimento:** com a padronização do fabricante escolhido, o SENAC SC garante o investimento anteriormente efetuado, pois os equipamentos mais novos já adquiridos pelo Senac SC são deste fabricante, o que convém com o princípio da economicidade;

    - **Garantia:** Embora a garantia solicitada neste TR seja pelo período de 5 anos do fornecedor, o fabricante da solução atual possui uma política de garantia que garante que após o anúncio de fim de fabricação do equipamento eles

ainda poderão ter a sua garantia renovada por no mínimo mais 5 anos, o que permite a utilização deste por um tempo maior, o que gera melhor custo/benefícios para o Senac SC;

- **Diminuição de "spare-parts":** A padronização dos equipamentos auxiliar facilita a administração, devido a utilização de apenas um sistema operacional em todos os equipamentos, ou seja, um único conjunto de comandos a serem utilizados para configuração de todos. Com isso, torna-se fácil o treinamento, a gestão do conhecimento, e auxiliar na redução do tempo de configuração e reparo. Este convém a citar o princípio a eficiência;

- **Desempenho:** Soluções de mesmo fabricante permite a utilização de recursos proprietários, ou seja, recursos que garantem maior desempenho dos equipamentos, mas que só podemos utilizá-los com a homogeneidade da malha;

- **Equipe de Administração:** com a padronização e a consequente simplificação, não há a necessidade de ampliar a equipe de administração, devido a redução da complexidade da administração e tempo de reparo, visto que hoje a equipe atual já conhece a tecnologia;

- **Backup/Restore:** caso haja necessidade de troca de algum equipamento, está se dará em tempo reduzido, pois será necessário apenas o tempo de troca física do equipamento no local e a rápida restauração das configurações através do software de gerenciamento;

- Assim posto, esta demanda implica na manutenção do padrão de equipamentos atualmente em uso, ou seja, a continuidade do produto da marca FORTINET. Cabe destacar, que essa manutenção pela marca FORTINET não implica em inexigibilidade de licitação, pois, existe no mercado uma quantidade considerável de empresas credenciadas pelo fabricante dos equipamentos capazes de fornecer os novos equipamentos e prestar os serviços desejados.

- Equipamentos de rede e segurança já existentes e em produção no SENAC SC:

Part Number	**Descrição**	**Serial Number**
FG-10-F100F-950-02-60	Firewall Fortigate 100F	FG100FTK19000952
FG-10-F100F-950-02-60	Firewall Fortigate 100F	FG100FTK19000649
FG-10-F100F-950-02-60	Firewall Fortigate 100F	FG100FTK19000957
FC2-10-M3004-248-02-60	Fortimanager 20 Dispositivos	FMG-VMTM19009493

4. CARACTERÍSTICAS MÍNIMAS DA SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

- A solução deverá estar devidamente licenciada por 60 meses para atender as funções, funcionalidades e serviços dos equipamentos ativos para no mínimo:
  - Controle de Aplicações;
  - Proteção IPS;
  - Proteção contra Ameaças Avançadas;
  - Filtro Web e de Conteúdo;
  - Análise de malwares modernos em nuvem do mesmo fabricante;
  - Roteamento inteligente de aplicações;
  - VPN site-to-site e client-to-site;
- A solução deve consistir em plataforma de proteção de rede baseada em equipamento físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source;
- Todos os equipamentos a serem fornecidos, bem como seu hardware e software, deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- Todos os modelos de Tipos de Firewalls ofertados, devem ser do mesmo fabricante e compatíveis com os todos itens de gerência centralizada e gerência de relatórios e logs;
- O equipamento deverá ser novo e sem uso anterior.
- O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada;
- O fabricante deve publicar as vulnerabilidades conhecidas em cada versão das plataformas NGFW e Gerenciamento, detalhar o meio de os meios de correções diante de um relatório PSIRT;
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- Por funcionalidades de Threat Prevention entende-se as seguintes funcionalidades habilitadas simultaneamente: Controle de aplicação, IPS (Intrusion Prevention System), Antimalware. Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;
- Para proteção do ambiente contra ataques cibernéticos, o dispositivo de proteção deve possuir módulo de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados no próprio appliance de NGFW;
- Deve implementar em um único dispositivo, de forma integrada, tecnologia de Next Generation Firewall com capacidade para filtro de pacotes, controle de aplicação, VPN IPSec e SSL, IPS, prevenção contra ameaça de vírus, spywares e

malwares e filtro de conteúdo/URL, além de haver integração com sandbox para prevenção contra ameaças avançadas;

- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI.
- Define-se o termo "appliance" como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço;
- Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de "appliance" que utilizam hardware e software de fabricantes diferentes;
- Todos os equipamentos appliances do tipo firewall ofertados, devem possuir homologação da ANATEL, emitida e válida no dia do certame/pregão.
- O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e via API.
- Deverá suportar tags de VLAN (802.1Q);
- Deverá possuir suporte a agregação de links via 802.3ad LACP;
- Deverá possuir ferramenta de diagnóstico do tipo "tcpdump" e ainda dispor de ferramenta integrada à interface web para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um software terceiro, tal como Wireshark;
- Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- Deverá possuir integração com tokens para autenticação de duplo fator;
- Deverá suportar single-sign-on;
- Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;
- Deverá suportar roteamento estático para IPv4 e IPv6;
- Deverá suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, OSPFv2, OSPFv3, BGP, RIP);
- Deverá suportar ECMP;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia, tais como: H.323 e SIP;
- Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo;
- Deverá permitir o funcionamento em modo transparente tipo "*bridge*";
- Deverá suportar PBR – Policy Based Routing;
- Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- Deverá possuir mecanismo de anti-spoofing;
- Deverá permitir criação de regras definidas pelo usuário;
- Deverá suportar sFlow ou Netflow;
- Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

- Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- Deverá permitir funcionamento em modo bridge em camada 2, roteador em camada 3, proxy explícito e sniffer via espelhamento;
- Deverá possuir mecanismo de tratamento de sessão (session-helpers ou ALGs);
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- Permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;
- Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e eventos de segurança;
- Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda 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;
- Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;
- Deverá possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;
- Deverá suportar ambientes multi-cloud;
- Deverá possuir a capacidade de criar automações através de gatilhos e ações, possibilitando uma atuação mais proativa;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- A configuração em alta disponibilidade deve sincronizar:
- Sessões;
- Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;
- Associações de Segurança das VPNs;
- Tabelas FIB;
- Assinaturas de IPS, Antivírus e AntiSpyware;
- A configuração de alta disponibilidade deve possibilitar monitoração de falha de link;
- As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
- Deverá possuir controle de acesso à Internet por endereço IP de origem e destino;
- Deverá possuir controle de acesso à Internet por subrede;
- Deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;
- Deverá suportar controles por zonas de segurança;
- Deverá suportar controles de políticas por porta e protocolo;
- Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

- Controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança;
- Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto, tal como uma subrede, por exemplo, ou seja, se a subrede não for 192.168.0.0/24, o tráfego deverá ser tratado.
- Controle, inspeção e de-criptografia de SSL por política para tráfego de saída;
- Deve ser possível realizar um espelhamento do tráfego de-criptografado.
- Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;
- A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos.
- 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;
- Deve suportar objetos de endereço IPv4 e IPv6 consolidados na mesma política de firewall
- Suporte a objetos e regras multicast;
- Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego.
- Deve ser possível criar política de firewall em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar logs de eventos.
- Deve possuir base com objetos contendo endereços IPs de serviços da Internet como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução.
- Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo.

- **FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES**

- Deverá reconhecer, no mínimo, 5000 (Cinco mil) aplicações com base na camada 7 do modelo OSI;
- Deverá permitir o monitoramento do tráfego de aplicações sem bloqueio de acesso aos usuários;

- Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
- Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- Deve ser possível bloquear aplicações detectadas em portas não comuns para aquela determinada aplicação.
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 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;
- Deverá atualizar a base de assinaturas de aplicações automaticamente;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve ser possível a criação de grupos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (BitTorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve ser possível limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- 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;
- Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet.
- Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP.

- **FUNCIONALIDADES DE IPS**

- Deverá permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- Deverá possuir integração à plataforma de segurança;
- Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas.
- Deve ser capaz de realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego.
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Possuir assinaturas para bloqueio de ataques de buffer overflow;
- Implementar os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo;
- Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento;
- Permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos;
- Deve ser possível criar políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos.
- Deve ser possível criar políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, Solaris, BSD, entre outros.
- Deve ser possível escanear e bloquear conexões a servidores de botnet.
- Deve dispor de opção para bloquear URLs maliciosas mediante base de dados local.
- Deve ser possível habilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS.
- Deve suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS.
- Deve suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros.
- Deve ser possível filtrar assinaturas com base no identificador CVE.
- Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um "wildcard" do CVE para abranger mais de um identificador;

- As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável.
- Deve incluir proteção contra ataques de negação de serviços;
- Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

- **FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS**

- Deverá possuir funções de antivírus e anti-spyware;
- Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;
- Deverá permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros);
- Deve dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a análise baseada em assinaturas.
- Deverá permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
- Deverá permitir o bloqueio de download de arquivos por tamanho;
- Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
- Deve dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros.
- Deve ser possível criar políticas de bloqueio de malware utilizando serviços de terceiros, onde o firewall receberá uma lista de hashes maliciosos.
- Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
- A solução de sandbox deve ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque;
- A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
- Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back;
- A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento;

- **FUNCIONALIDADES DE FILTRO WEB E CONTEÚDO**

- Deverá permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- Deverá possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
- 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;
- Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deverá possuir a função de exclusão de URLs do bloqueio;
- Deverá permitir a customização de página de bloqueio;
- Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
- Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário.
- Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego.
- Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website.
- Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado.
- Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos;
- Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo.
- Deverá permitir além do Web Proxy explícito, suportar proxy Web transparente.

- **IDENTIFICAÇÃO DOS USUÁRIOS**

- 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;
- 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;
- Deve possuir integração e suporte a Microsoft Active Directory para, no mínimo, o sistema operacional Windows Server 2012 R2;

- 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 SSO (Single Sign-On). Essa funcionalidade não deve possuir limites quanto a licenciamento de usuários;
- Deve possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a Internet para que antes de iniciar a navegação, apresente-se um portal de autenticação residente no firewall do tipo portal cativo;
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix, VMware Horizon e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

- **FUNCIONALIDADES DE VPN**

- Suportar VPN Site-to-Site e Client-to-Site;
- Suportar IPSec VPN;
- Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- A VPN IPSec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- A VPN IPSec deverá suportar autenticação MD5, SHA1, SHA256, SHA384 e SHA512;
- A VPN IPSec deverá suportar Diffie-Hellman Grupos 1, 2, 5 e 14, Grupos 15 à 21 e Grupos 27 à 32;
- A VPN IPSec deve suportar algoritmo Internet Key Exchange (IKE v1 e v2);
- Deverá permitir habilitar e desabilitar túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas;
- A VPN IPSec deve suportar Forward Error Correction (FEC);
- Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;
- Deverá possuir suporte a VPNs IPSec Site-to-Site e VPNs IPSec Client-to-Site;
- A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento e por meio de portal web;
- Deverá possuir suporte a VPN SSL e deverá manter uma conexão segura com o portal durante a sessão;
- 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;
- A VPN SSL deve dispor de função que transite pelo túnel somente as subredes corporativas, ao passo que o acesso à Internet deve ocorrer diretamente pela estação do usuário remoto.

- Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- Solução deverá ser capaz de prover uma arquitetura similar ao conceito de Auto Discovery VPN – ADVPN;
- Deve suportar NAT Traversal;
- A VPN IPSec deve ser compatível com ambiente em alta disponibilidade garantindo que o tráfego de VPN não sofrerá interrupção durante um evento de HA.
- Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- O agente de VPN SSL ou IPSec client-to-site, o qual deve ser do mesmo fabricante do Firewall, deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8/8.1 (32 e 64 bit), Windows 10 (32 e 64 bit), Windows 11 (64 bit), Mac OS X (v10.15 ou superior), Ubuntu 18.04 ou superior, RedHat 7.4 ou superior, CentOS 7.4 ou superior.
- Deve ser possível realizar algumas verificações da estação do usuário durante a conexão de VPN, tais como verificações de sistema operacional, antivírus habilitado, firewall habilitado, processo rodando e validação de chave de registro.

- **FUNCIONALIDADES DE ROTEAMENTO INTELIGENTE DE APLICAÇÃO**

- A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- Deverá ser capaz de agregar pelo menos 03 (três) links em uma interface virtual;
- A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de verificações de saúde dos links WAN, permitindo testes de resposta por PING, HTTP, TCP/UDP ECHO, DNS e TWAMP. Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
- 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;
- 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;
- Deve suportar o uso de VRF (Virtual Routing and Forwarding);
- A solução de deve possuir suporte a Policy Based Routing ou Policy Based Forwarding;
- Deve suportar roteamento estático e dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- Deverá poder adicionar e equilibrar, no mínimo, 06 interfaces de dados (links e VPNs);
- Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- Deverá permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da interface virtual;

- Deve desempenhar a função de duplicidade de pacote permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não ocorrer retransmissão;
- Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;
- Deve permitir configurar o código de DiffServ (DSCP) do pacote ESP do túnel IPSec;
- Deverá permitir marcar com DSCP os testes de link para obter uma avaliação mais realista da qualidade de um determinado link;
- Deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:
- Número de Sessões,
- Volume de Tráfego,
- IP de Origem e Destino;
- Transbordo de Link baseado em limite de banda.
- As regras de escolha de roteamento devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de origem e destino e serviços de Internet.
- Deve permitir a customização dos tempos para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido.
- A solução de deve prover estatísticas em tempo real na interface web a respeito da ocupação de banda (upload e download) e desempenho das verificações de saúde (perda de pacote, jitter e latência);
- Deve ser possível configurar a porcentagem de perda de pacote e o tempo de latência e jitter na verificação de estado de saúde do link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
- Deve dispor de opção que maximize o uso da largura de banda utilizando os links WANs que estejam dentro do nível de saúde estipulado.
- Deve ser possível monitorar a saúde do link de modo passivo, sem a emissão de pacotes de verificação, utilizando somente informações das sessões que transitam pelo equipamento.
- Deve ser possível utilizar o método de verificação de saúde passivo na existência de tráfego e ativo na inexistência de tráfego.
- Deve suportar balanceamento de tráfego por sessão e pacote;
- Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.
- Deve suportar algum método de descoberta automática de VPN, funcionalidade esta que tem o intuito de dinamicamente viabilizar que túneis sejam estabelecidos entre duas localidades remotas, sem necessidade do tráfego transitar pelo ponto central conhecido por HUB.

- **QUALITY OF SERVICE (QOS)**

- Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, BitTorrent, etc) e ter um alto consumo de largura de banda, 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 largura de banda máxima quando forem solicitadas por diferentes usuários ou aplicações.
- Deve suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
  - por endereço de origem;
  - por endereço de destino;
  - por usuário e grupo;
  - por aplicações;
  - por protocolo e porta;
  - por categoria de URL;
- O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 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, entre outros;
- 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;
- O QoS deve possibilitar a definição de fila de prioridade;
- Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o vínculo com categorias de URL, IPs de origem e destino, grupos de usuários, protocolos e portas;
- Deve ter a capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas e mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
- Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que tiverem correspondência na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que tiverem correspondência na regra;
- Deve possibilitar a definição de bandas distintas para download e upload;

- **CARACTERÍSTICAS REFERENTES A NGFW RESERVAS**

- A solução deverá estar devidamente licenciada por 60 meses para atender as funções, funcionalidades e serviços dos equipamentos reservas para no mínimo:
- Controle de Aplicações;
- Atualização da base de dados de IPs geográficos;
- Serviços de Internet SaaS;
- DDNS;
- Garantia e suporte remoto diretamente com o fabricante na modalidade de 24x7;
- A solução deve consistir em plataforma de proteção de rede baseada em equipamento físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source;

- Todos os equipamentos a serem fornecidos, bem como seu hardware e software, deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- Todos os modelos de Tipos de Firewalls ofertados, devem ser do mesmo fabricante e compatíveis com os todos itens de gerência centralizada e gerência de relatórios e logs;
- O equipamento deverá ser novo e sem uso anterior.
- O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada;
- O fabricante deve publicar as vulnerabilidades conhecidas em cada versão das plataformas NGFW e Gerenciamento, detalhar o meio de os meios de correções diante de um relatório PSIRT;
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- Por funcionalidades de Threat Prevention entende-se as seguintes funcionalidades habilitadas simultaneamente: Controle de aplicação, IPS (Intrusion Prevention System), Antimalware. Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI.
- Define-se o termo "appliance" como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço;
- Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de "appliance" que utilizam hardware e software de fabricantes diferentes;
- Todos os equipamentos appliances do tipo firewall ofertados, devem possuir homologação da ANATEL, emitida e válida no dia do certame/pregão.

- **FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES**

- Deverá reconhecer, no mínimo, 5000 (Cinco mil) aplicações com base na camada 7 do modelo OSI;
- Deverá permitir o monitoramento do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

- Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- Deve ser possível bloquear aplicações detectadas em portas não comuns para aquela determinada aplicação.
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 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;
- Deverá atualizar a base de assinaturas de aplicações automaticamente;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve ser possível a criação de grupos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (BitTorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve ser possível limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- 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;
- Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet.
- Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP.

5. DO QUANTITATIVO E DESCRITIVO DOS OBJETOS

Quantidade total a ser registrada:

LOTE 01

Item	Descritivo	Unid.	Qtd.	Part Number
01	Firewall Fortigate 40F	Unidade	06	FG-40F
02	Licença para Fortigate 40F - UTP	Unidade	05	FC-10-0040F-950-02-60
03	Licença Forticare para Fortigate 40F	Unidade	01	FC-10-0040F-314-02-60
04	Firewall Fortigate 60F	Unidade	09	FC-60F
05	Licença para Fortigate 60F - UTP	Unidade	08	FC-10-0060F-950-02-60
06	Licença Forticare para Fortigate 60F	Unidade	01	FC-10-0060F-314-02-60
07	Firewall Fortigate 100F	Unidade	10	FC-100F
08	Licença para Fortigate 100F - UTP	Unidade	10	FC-10-F100F-950-02-60
09	Firewall Fortigate 120G	Unidade	06	FC-120G
10	Licença para Fortigate 120G - UTP	Unidade	05	FC-10-F120G-950-02-60
11	Licença Forticare para Fortigate 120G	Unidade	01	FC-10-0120G-247-02-60
12	Licença FortiAnalyzer – Subscrição	Unidade	06	FC1-10-AZVMS-465-01-60
13	Licença Forticare Premium Fortimanager 1-110	Unidade	01	FC2-10-M3004-248-02-60
14	Licença Fortimanager Perpétua 10 Upgrade	Unidade	01	FMG-VM-10-UG
15	Licença Coterm FG100FTK19000952 UTP	Unidade	01	COTERM
16	Licença Coterm FG100FTK19000957 UTP	Unidade	01	COTERM
17	Licença Coterm FG100FTK19000649 FORTICARE	Unidade	01	COTERM
18	Serviços de instalação remota	Unidade	01	-
19	Banco de Horas – 300 horas	Unidade	01	-

5. DAS ESPECIFICAÇÕES TÉCNICAS/EXECUÇÃO DOS SERVIÇOS

5.1. Das Especificações Técnicas:

LOTE 1 – ITEM 01: FORTINET FORTIGATE 40F

Especificações técnicas mínimas:

- Deve suportar, no mínimo, 04 (quatro) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- Deve suportar, no mínimo, 600.000 (seiscentos mil) conexões simultâneas;
- Deve suportar, no mínimo, 30.000 (trinta mil) novas conexões por segundo;

- Deve Suportar, no mínimo, 04 (quatro) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de clientes VPN IPSEC simultâneos;
- Deve suportar, no mínimo, 450 (quatrocentos e cinquenta) Mbps de throughput de VPN SSL;
- Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultâneos;
- Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 300 (trezentos) Mbps de throughput de Inspeção SSL;
- Deve suportar, no mínimo, 600 (seiscentos) Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.
- Deve possuir, pelo menos, 05 (cinco) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve estar licenciado para gerenciar no mínimo 08 (oito) switches e 16 (dezesseis) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance.

LOTE 1 – ITEM 02: LICENÇA PARA FORTIGATE 40F

Especificações técnicas mínimas:

- Licenciamento UTP – IPS, Anti-Malware Protection, URL, DNS e Video Filtering, Anti-SPAM com Forticare Premium pelo período de 60 meses.

LOTE 1 – ITEM 03: LICENÇA PARA FORTIGATE 40F - FORTICARE

Especificações técnicas mínimas:

- Garantia Fortinet FortiCare Premium pelo período de 60 meses.

LOTE 1 – ITEM 04: FORTINET FORTIGATE 60F

Especificações técnicas mínimas:

- Deve suportar, no mínimo, 05 (cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

- Deve suportar, no mínimo, 700.000 (setecentos mil) conexões simultâneas;
- Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;
- Deve suportar, no mínimo, 06 (seis) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 400 (quatrocentos) túneis de clientes VPN IPSEC simultâneos;
- Deve suportar, no mínimo, 800 (oitocentos) Mbps de throughput de VPN SSL;
- Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultâneos;
- Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 600 (seiscentos) Mbps de throughput de Inspeção SSL;
- Deve suportar, no mínimo, 700 (setecentos) Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.
- Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve estar licenciado para gerenciar 60 (sessenta) pontos de acesso sem fio e 20 (vinte) switches simultaneamente em um único appliance;
- Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

LOTE 1 – ITEM 05: LICENÇA PARA FORTIGATE 60F

Especificações técnicas mínimas:

- Licenciamento UTP – IPS, Anti-Malware Protection, URL, DNS e Video Filtering, Anti-SPAM com Forticare Premium pelo período de 60 meses.

LOTE 1 – ITEM 06: LICENÇA PARA FORTIGATE 60F - FORTICARE

Especificações técnicas mínimas:

- Garantia Fortinet FortiCare Premium pelo período de 60 meses.

LOTE 1 – ITEM 07: FORTINET FORTIGATE 100F

Especificações técnicas mínimas:

- Deve suportar, no mínimo, 10 (dez) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- Deve suportar, no mínimo, 1.5 Milhão (um milhão e quinhentas mil) conexões simultâneas;
- Deve suportar, no mínimo, 50.000 (cinquenta mil) novas conexões por segundo;

- Deve suportar, no mínimo, 10 (dez) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de clientes VPN IPSEC simultâneos;
- Deve suportar, no mínimo, 01 (um) Gbps de throughput de VPN SSL;
- Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;
- Deve suportar, no mínimo, 02 (dois) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 01 (um) Gbps de throughput de Inspeção SSL;
- Deve suportar, no mínimo, 01 (um) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.
- Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve possuir, pelo menos, 08 (oito) interfaces Gigabit Ethernet com conectores SFP;
- Deve possuir, pelo menos, 02 (duas) interfaces 10 Gigabit Ethernet com conectores SFP+;
- Deve estar licenciado para gerenciar no mínimo 30 (trinta) switches e 120 (cento e vinte) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve possuir fonte de alimentação AC redundante;
- Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

LOTE 1 – ITEM 08: LICENÇA PARA FORTIGATE 100F

Especificações técnicas mínimas:

- Licenciamento UTP – IPS, Anti-Malware Protection, URL, DNS e Video Filtering, Anti-SPAM com Forticare Premium pelo período de 60 meses.

LOTE 1 – ITEM 09: FORTINET FORTIGATE 120G

Especificações técnicas mínimas:

- Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- Deve suportar, no mínimo, 2,5 (dois vírgula cinco) milhões de conexões simultâneas;
- Deve suportar, no mínimo, 130.000 (cento e trinta mil) novas conexões por segundo;
- Deve suportar, no mínimo, 35 (trinta e cinco) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC Site-to-Site simultâneos;

- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de clientes VPN IPSEC simultâneos;
- Deve suportar, no mínimo, 1,4 (um vírgula quatro) Gbps de throughput de VPN SSL;
- Deve suportar, no mínimo, 400 (quatrocentos) clientes de VPN SSL simultâneos;
- Deve suportar, no mínimo, 5 (cinco) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 3 (três) Gbps de throughput de Inspeção SSL;
- Deve suportar, no mínimo, 2,5 (dois vírgula cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.
- Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores SFP;
- Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet com conectores SFP+;
- Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
- Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;
- Deve estar licenciado para gerenciar no mínimo 45 (quarenta e cinco) switches e 120 (cento e vinte) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve possuir fonte de alimentação AC redundante;
- Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

LOTE 1 – ITEM 10: LICENÇA PARA FORTIGATE 120G

Especificações técnicas mínimas:

- Licenciamento UTP – IPS, Anti-Malware Protection, URL, DNS e Video Filtering, Anti-SPAM com Forticare Premium pelo período de 60 meses.

- **LOTE 1 – ITEM 11: LICENÇA PARA FORTIGATE 120G - FORTICARE**

Especificações técnicas mínimas:

- Garantia Fortinet FortiCare Premium pelo período de 60 meses.

LOTE 1 – ITEM 12: LICENÇA FORTIANALYZER PARA 30GB DIA PARA 60 MESES

Especificações técnicas mínimas:

- A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução de firewalls e ter como objetivo a coleta, armazenamento e análise automatizada de registros em modo centralizado de todos os equipamentos a partir de uma única console de administração.
- Poderá ser entregue em formato de appliance físico ou appliance virtual;
- Deverá estar devidamente licenciada para:
- Suportar a coleta de, no mínimo, 30 GB de logs diários;
- O formato de licenciamento deverá permitir o aumento gradativo, em formato de add on, de modo que o SENAC SC aumente seu parque de equipamentos de comutação de acordo com as quantidades totais do certame em questão;
- Caso a solução seja entregue como appliance virtual, este deve suportar:
- Deve ser compatível com os hypervisor VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM;
- Não deverá existir limite para o número de vCPUs no appliance virtual;
- Não deverá existir limite para a expansão da memória RAM no appliance virtual;
- Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
- Realizar o backup das configurações para permitir o retorno de uma configuração salva;
- Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
- Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
- Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;
- Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;
- Utilizar técnicas de machine learning para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;
- Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;
- Deve oferece um portal do cliente fácil de usar, permitindo monitoramento de

políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;

- Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
- Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
- Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
- Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
- Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
- Deve possuir mecanismos de remoção automática para logs antigos;
- Permitir importação e exportação de relatórios
- Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;
- Deve permitir exportar os logs no formato CSV;
- Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- 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;
- A solução deve ter relatórios predefinidos;
- Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
- Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
- Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
- Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
- Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
- Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
- Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
- Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução,

exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

- Permitir o envio por e-mail relatórios automaticamente;
- Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;
- Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
- Deve permitir o uso de filtros nos relatórios;
- Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- Permitir especificar o idioma dos relatórios criados;
- Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
- Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
- Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
- Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- Deve permitir visualizar em tempo real os logs recebidos;
- Deve permitir o encaminhamento de log no formato syslog;
- Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
- Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
- Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;
- Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição;
- Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o malware e quais são os autores;

- Deve permitir gerar alertas de eventos a partir de logs recebidos;
- Deve suportar o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas;

LOTE 1 – ITEM 13: LICENÇA PARA FORTIMANAGER - FORTICARE

Especificações técnicas mínimas:

- Garantia Fortinet FortiCare Premium Support (1 - 110 devices/virtual domains) pelo período de 60 meses.

LOTE 1 – ITEM 14: LICENÇA DE UPGRADE FORTIMANAGER

Especificações técnicas mínimas:

- Deverá estar devidamente licenciada para:
- Gerenciar, no mínimo, 10 unidades dos equipamentos da solução de segurança firewall/sdwan de forma simultânea (licença será adicionada a licença existente que será disponibilizada pela CONTRATANTE)
- O formato de licenciamento deverá permitir o aumento gradativo, em formato de add on, de modo que o IFPI aumente seu parque de equipamentos de comutação de acordo com as quantidades totais do certame em questão;
- Caso a solução seja entregue como appliance virtual, este deve suportar:
- Deve ser compatível com os hypervisor VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM;
- Não deverá existir limite para o número de vCPUs no appliance virtual;
- Não deverá existir limite para a expansão da memória RAM no appliance virtual;
- Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
- 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;
- Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
- Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no

mesmo ativo;

- Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas;
- Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;
- Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;
- Permitir usar palavras chaves ou cores para facilitar identificação de regras;
- Permitir localizar em quais regras um objeto (ex. computador, serviço etc.) está sendo utilizado;
- Permitir criação de regras que fiquem ativas em horário definido;
- Permitir criação de regras com data de expiração;
- Realizar o backup das configurações para permitir o retorno de uma configuração salva;
- Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
- Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
- Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;
- Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
- Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ ou PKI.
- Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;
- Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;
- Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;
- Deve oferece um portal do cliente fácil de usar, permitindo monitoramento de

políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;

- Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
- A gerência centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento de gerenciamento centralizado, ou fornecido em equipamento externo do mesmo fabricante;
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- Deve suportar a configuração Master / Slave de alta disponibilidade em camada

LOTE 1 – ITEM 15: COOTERM LICENÇA FIREWALL

Especificações técnicas mínimas:

- Coterm 6039838-1 - Licença UTP (DE 25/11/2025 ATÉ 01/04/2030) para Firewall SN: FG100FTK19000952.

LOTE 1 – ITEM 16: COOTERM LICENÇA FIREWALL

Especificações técnicas mínimas:

- Coterm 6039838-1 - Licença UTP (DE 25/11/2025 ATÉ 01/04/2030) para Firewall SN: FG100FTK19000957.

LOTE 1 – ITEM 17: COOTERM LICENÇA FIREWALL - FORTICARE

Especificações técnicas mínimas:

- Coterm 6039838-1 - Forticare Premium (DE 25/11/2025 ATÉ 01/04/2030) para Firewall SN: FG100FTK19000649.

LOTE 1 – ITEM 18: SERVIÇO DE PROJETO E CONFIGURAÇÃO DA SOLUÇÃO

Especificações técnicas mínimas para instalação de FORTIGATE:

- Os serviços de instalação física serão de responsabilidade da CONTRATANTE.
- Os serviços de configuração e ativação lógica dos equipamentos pode ser feito de forma remota.
- O conjunto de itens (Equipamentos e Licenças) será considerado instalado e ativo somente após o perfeito funcionamento, a finalização das orientações à equipe

técnica e do ateste técnico por parte do Gestor do Contrato;

- São de responsabilidade da CONTRATADA, entre outras atividades:
- Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos firewalls em produção no ambiente atual (PfSense) para a nova solução;
- Configurar as funcionalidades relevantes a implementação da solução como: Endereçamento, VLANs, LACP, DHCP e tipos NAT;
- Configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF;
- Realizar a configuração das políticas analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários e grupos de usuários;
- Implementar políticas de bloqueios;
- Configurar limitações de banda com base no IP de origem, usuários e grupos;
- Configurar regras de IPS, Anti-Malware e Filtro URL nos equipamentos de NGFW;
- Configurar regras de gestão de links, balanceamento, políticas de SD-WAN;
- Rollout de unidades Remotas - Instalação rápida e automatizada, utilizarão a tecnologia ZTP (Zero Touch Provisioning);
- O Provisionamento Zero Toque da solução de Segurança e SD-WAN Fortinet permite um tipo de implementação simples e automatizada, exigindo do técnico de campo, apenas o conhecimento básico de cabeamento e comunicação de rede.
- O processo de ZTP segue as seguintes etapas:
    1. O FortiGate recebe DHCP em sua interface WAN e ganha acesso à internet;
    2. Utiliza o acesso à internet para se comunicar com os servidores de registro da Fortinet;
    3. Após realizar o registro, recebe a informação do endereço IP ou nome alcançável do FortiManager responsável por sua configuração;
    4. Entra em contato com o FortiManager;
    5. Inicia o processo de autorização e atualização;
    6. Recebe os templates de provisionamento de acordo com o perfil ao qual seu número de série ou modelo foi associado.
- Os serviços de instalação deverão ser executados pela CONTRATADA, durante o horário comercial compreendido entre 8h e 18h, 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.
- 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;

- 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;
- A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da CONTRATANTE, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;
- Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI;
- 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;
- O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia;
- A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes se constitui em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta;
- Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação:
- Aspecto da arquitetura implantada;
- Configuração;
- Descrição das características e recursos utilizados;
- Testes e integração dos ambientes de redes locais da instalação;
- A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;
- A documentação poderá ser entregue em via impressa ou meio digital;
- A documentação deverá validada pela equipe técnica da CONTRATANTE;
- Toda informação manuseada durante a instalação, configuração e testes são de

uso restrito da CONTRATANTE. A CONTRADADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;

Especificações técnicas mínimas para instalação de FORTIANALYZER:

- Os serviços de instalação, configuração e ativação lógica dos equipamentos será feito de forma remota.
- O conjunto de itens (Equipamentos e Licenças) será considerado instalado e ativo somente após o perfeito funcionamento, a finalização das orientações à equipe técnica e do ateste técnico por parte do Gestor do Contrato;
- Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 18h, 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;
- 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;
- 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;
- A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;
- Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI;
- 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;
- O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período

de garantia;

- A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes se constitui em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta;
- Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação:
- Aspecto da arquitetura implantada;
- Configuração;
- Descrição das características e recursos utilizados;
- Testes e integração dos ambientes de redes locais da instalação;
- A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;
- A documentação poderá ser entregue em via impressa ou meio digital;
- A documentação deverá validada pela equipe técnica da CONTRATANTE;
- Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRADADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários

Especificações técnicas mínimas para instalação de FORTIMANAGER:

- Os serviços de instalação física serão de responsabilidade da CONTRATANTE (instâncias existentes) com orientação e apoio da CONTRATADA.
- Os serviços de configuração e ativação lógica dos equipamentos pode ser feito de forma remota.
- O conjunto de itens (Equipamentos e/ou Licenças) será considerado instalado e ativo somente após o perfeito funcionamento, a finalização das orientações à equipe técnica e do ateste técnico por parte do Gestor do Contrato;
- Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 18h, 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;
- 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;

- 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;
- A CONTRATADA deverá elaborar Relatório de Instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;
- Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI;
- 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;
- O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia;
- A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes se constitui em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta;
- Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a "DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO" contendo todas as informações da implantação:
- Aspecto da arquitetura implantada;
- Configuração;
- Descrição das características e recursos utilizados;
- Testes e integração dos ambientes de redes locais da instalação;
- A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;
- A documentação poderá ser entregue em via impressa ou meio digital;
- A documentação deverá validada pela equipe técnica da CONTRATANTE;
- Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRADADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários

LOTE 1 – ITEM 19: BANCO DE HORAS

Especificações técnicas mínimas:

- Exigências para o Colaborador Responsável:
- Certificação Técnica Específica: O colaborador responsável pela configuração dos equipamentos deve possuir certificação FORTINET CERTIFIED PROFESSIONAL ou superior.
- Atualização e Conhecimento Contínuo: Manter-se atualizado com as melhores práticas de segurança e tendências de redes para garantir a qualidade e confiabilidade da configuração.

Suporte de Firewalls

- Os serviços de suporte para firewalls incluem, mas não se limitam a:
- Configuração inicial e customização de políticas de segurança.
- Gerenciamento de atualizações de firmware e patches.
- Análise de logs de segurança.
- Configuração de VPNs (site-to-site e client-to-site).
- Suporte em incidentes de segurança e resposta a ataques.
- Configuração de regras de controle de acesso e IPS/IDS.
- Integração com soluções de autenticação como LDAP e Active Directory.
- Suporte para implementação de soluções SD-WAN.
- Configuração de funcionalidades de filtro de conteúdo e controle de aplicações.
- Testes de desempenho e ajustes para throughput e inspeção SSL.
- Deverá existir acesso ao serviço de assistência técnica do fabricante por telefone gratuito, e-mail ou acesso seguro ao site, 8 (oito) horas por dia, 7 (sete) dias por semana, em horário comercial.
- Deverá existir acesso ao serviço de assistência técnica da CONTRATADA por meio de telefone gratuito, e-mail ou acesso ao site, 8 (oito) horas por dia, 7 (sete) dias por semana, em horário comercial.
- Além disso, a CONTRATADA deverá disponibilizar um sistema de gerenciamento de chamados, que permita à CONTRATANTE:
- Abrir solicitações de suporte técnico;
- Acompanhar o status dos chamados em tempo real;
- Registrar históricos de atendimento;
- Obter atualizações sobre a resolução de problemas;
- Monitorar e contabilizar automaticamente os tempos de atendimento e resolução (SLA), de acordo com os níveis de serviço estabelecidos no contrato.

- O atendimento a chamados técnicos deverá ser realizado em horário comercial obedecendo as condições de acordo com o SLA.
- A indisponibilidade da comunicação por parte da CONTRATADA não afetará a contagem de tempo relativa aos prazos de atendimento previamente acordados. O sistema de chamados deverá ser acessível via internet, com autenticação segura, garantindo a transparência e a eficiência no processo de suporte técnico, bem como o cumprimento dos SLAs acordados.
- Os chamados junto à CONTRATADA deverão ser atendidos por profissionais da CONTRATADA, em português brasileiro e serão usados para abrir solicitações.

SLA (Service level Agreement)

O SLA (Service Level Agreement) dos atendimentos será tratado de acordo com o nível de severidade da ocorrência, conforme indicadores a seguir:

- Prioridade 01 – Crítica

O serviço está fora de operação ou há um impacto crítico sobre a operação.

- Prioridade 02 - Alta

A operação do serviço está seriamente degradada ou o desempenho inaceitável do serviço está causando impacto negativo sobre aspectos significativos da operação.

- Prioridade 03 - Média

O desempenho operacional do serviço está prejudicado, embora a maioria das operações usuais ainda esteja funcionando.

- Prioridade 04 - Baixa

Há necessidade de informações ou assistência relacionadas a recursos, instalação ou configuração dos serviços. Claramente, há pouco ou nenhum impacto sobre a operação.

Após o contato da CLIENTE da abertura de chamado, os serviços serão tratados e atendidos conforme SLA (Service Level Agreement) nas seguintes categorias de prioridades:

Prioridade	**Atendimento**	**Tempo de Resposta**
P01 – Crítica	15 Minutos	01 Hora
P02 – Alta	15 Minutos	02 Horas
P03 – Média	15 Minutos	04 Horas
P04 – Baixa	15 Minutos	08 Horas

O SLA (Service Level Agreement) referente ao tempo de atendimento, é

contado a partir da abertura do chamado de incidente.

O prazo para resposta a incidentes é válido apenas para soluções no escopo do SIEM fornecido pela contratada ou para casos que envolvam incidentes pertinentes à solução fornecida pela CONTRATADA. A contabilização do tempo de atendimento só será válida quando a resolução depender questões pertinentes aos serviços/SLAs contratados, ou seja, excetuam-se os incidentes de situações como quedas de links, falta de energia, problemas físicos da infraestrutura do cliente, falhas de hardware, bugs de software dos fabricantes sem correções disponíveis e tudo mais que depender de terceiros e estiver fora do alcance da CONTRATADA.

É importante, também, ressaltar que o tempo de atendimento/resposta definido neste documento possui foco nos chamados de resolução de incidentes, não abrangendo chamados de requisição de serviço (solicitações) ou resolução de problema (análises de causa).

Os SLAs (Service Level Agreement) são contados a partir do momento de abertura do chamado. Sendo o prazo para resposta de incidente válido apenas para casos que envolvam problemas pertinentes a CONTRATADA, sendo excluídos os casos que envolvam falhas de hardware ou de força maior. O acionamento terá que ser feito dentro do período de atendimento.

Nos SLAs acima não está incluso as atividades das fases de mitigação, contenção, recolhimento de evidências, comunicação, documentação, recuperação e restauração.

Utilização e Pagamento de Horas Contratadas:

- A CONTRATANTE não está obrigada a utilizar integralmente as 300 (trezentas) horas de suporte técnico contratadas para os equipamentos de Rede e Segurança durante a vigência do contrato. O uso das horas será realizado conforme a necessidade e conveniência da CONTRATANTE.
- O pagamento das horas contratadas será efetuado conforme a demanda efetivamente utilizada, ou seja, a CONTRATANTE somente realizará o pagamento pelas horas de suporte que forem efetivamente solicitadas e prestadas pela CONTRATADA, respeitando os valores unitários previamente definidos no contrato.
- Fica estabelecido que eventuais horas não utilizadas ao final da vigência do contrato não gerarão qualquer ônus, obrigação de compensação ou reembolso financeiro por parte da CONTRATANTE à CONTRATADA. A CONTRATANTE possui plena discricionariedade para determinar o volume de horas que serão aplicadas, sem prejuízo às condições contratuais.

Atendimento:

- O atendimento referente às horas de suporte técnico contratadas poderá ser realizado de forma remota.
- A escolha da modalidade será definida pela CONTRATANTE, considerando a natureza do problema, a urgência do atendimento e a viabilidade técnica da

solução. A CONTRATADA deverá estar apta a prestar suporte em ambas as modalidades, garantindo que o atendimento seja realizado de maneira eficiente e dentro dos prazos previamente acordados.

- Eventuais deslocamentos necessários para atendimento presencial deverão ser previamente autorizados pela CONTRATANTE, e os custos associados estarão sujeitos às condições estabelecidas no contrato.

6. EXIGÊNCIAS COMERCIAIS, TÉCNICAS E DE QUALIFICAÇÃO DO FORNECEDOR

Especificações técnicas mínimas:

- Deve ser emitida uma declaração do Fabricante (FORTINET), por meio de representantes no Brasil, em papel timbrado, garantindo que a empresa revendedora está apta a comercializar todo o suporte, garantia, produtos e licenças ofertadas no edital.
- Deve fornecer declaração que comprova que é Revenda autorizada da Fortinet no Brasil no nível "Select Partner", "Advanced Partner" ou "Expert Partner". A validação deve ser possível por meio do site oficial da Fortinet: "https://partnerportal.fortinet.com/directory/search?l=Brazil"
- Deverá ser fornecido atestados de capacidade técnica fornecidos por pessoas jurídicas de direito público ou privado, impresso em papel timbrado, com os dados do responsável pela informação atestada, comprovando que a licitante forneceu, instalou, configurou e prestou suporte técnico em solução de SD Wan e Segurança e sistema de gestão centralizada de controle de redes de quantidade igual ou superior ao deste certame;
- Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante.
- O licitante 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 foram prestados os serviços, entre outros documentos.
- Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.
- A exigência de atestado de capacidade técnica operacional é necessária para assegurar que a CONTRATADA possua experiência e competência comprovada na execução dos serviços demandados, garantindo a qualidade, segurança e eficiência na prestação dos serviços, minimizando riscos de falhas operacionais e garantindo a continuidade dos serviços conforme as especificações deste Termo de Referência.
- A seu critério, a entidade poderá fazer diligências para comprovação do conteúdo dos atestados. Não serão aceitas declarações genéricas de catálogos, manuais ou internet. Os atestados deverão ser apresentados em seu original ou cópia devidamente autenticada.
- Fica expressamente vedada a subcontratação, total ou parcial, dos serviços

objeto desse edital, incluindo, mas não limitado à instalação, configuração, ativação e suporte da solução contratada. A execução dos serviços deverá ser realizada exclusivamente por equipe da empresa licitante, com comprovação de vínculo profissional dos técnicos envolvidos.

7. DA ENTREGA E PAGAMENTO DOS EQUIPAMENTOS, LICENÇAS E INSTALAÇÃO REMOTA

A entrega dos equipamentos deverá ser feita no Setor de Tecnologia da Informação e Comunicação do Departamento Regional do Senac Santa Catarina, localizado na Rua Felipe Schmidt, 785, 7º Andar – Centro – Florianópolis – SC CEP: 88010-002.

A entrega das licenças deverá ser feita digitalmente através de endereço de correio eletrônico a ser informado posteriormente conforme procedimento do fabricante.

O pagamento dos equipamentos, licenças e da instalação remota, objetos desse termo de referência, será realizado 30 (trinta) dias após a conclusão da Instalação Remota.

8. TRANSFERÊNCIA DE CONHECIMENTO

No decorrer, ou ao final da entrega e implementação da solução de firewall, a empresa contratada deverá realizar a transferência de conhecimento para a equipe técnica designada pela contratante. Essa transferência deverá contemplar, no mínimo:

- Apresentação detalhada da arquitetura implementada, incluindo configurações realizadas, políticas de segurança aplicadas e integrações com outros sistemas;
- Demonstração prática das funcionalidades principais do equipamento e do sistema de gerenciamento;
- Orientações sobre procedimentos de operação, monitoramento, manutenção preventiva e corretiva;
- Entrega de documentação técnica atualizada, contendo manuais, diagramas, procedimentos e boas práticas;
- Sessão de treinamento presencial ou remoto, com duração mínima de 20 (vinte) horas, com possibilidade de esclarecimento de dúvidas.

Florianópolis, 12 de setembro de 2025

Setor de Tecnologia da Informação e Comunicação.

PREGÃO ELETRÔNICO N. 30/2025

LICITAÇÃO N. 1079455

ANEXO II – ACEITAÇÃO DAS CONDIÇÕES DO EDITAL

A empresa....., inscrita no CNPJ ....., representada por ....., declara, para os devidos fins, que tomou conhecimento e examinou, cuidadosamente, o Edital e os respectivos anexos do Pregão Eletrônico n. 30/2025 do **Senac/SC**, para contratação do objeto desta licitação e de ter integralmente compreendido e aceito as condições nele estabelecidas.

Declara ainda que:

1. Não possui no quadro societário dirigente ou empregado do **Senac/SC.**
2. Não se encontra em processo falência ou dissolução.
3. Não foi punida com suspensão do direito de contratar ou licitar com o **Senac/SC.**
4. Não figura como sociedade integrante de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, desde que, em diligências, se comprove o conluio entre eles com intuito de frustrar a competitividade do certame.
5. Não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e nem menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos.
6. Está ciente e concorda com as disposições previstas no Edital, inclusive acerca da Proteção de Dados Pessoais, em atendimento à Lei 13.709/2018.

Florianópolis, ... de ..... de 2025.

_____

(nome do representante legal/contratual da empresa)

OBSERVAÇÃO:
Este documento deverá ser obrigatoriamente preenchido em papel timbrado da licitante e estar devidamente assinado eletronicamente por seu representante legal.

PREGÃO ELETRÔNICO N. 30/2025

LICITAÇÃO N. 1079455

ANEXO III –MODELO DE PROPOSTA

Ao
SENAC – Serviço Nacional de Aprendizagem Comercial
Administração Regional em Santa Catarina
A/C.: Comissão Permanente de Licitação
Rua Felipe Schmidt, 785, 7º Andar - Centro – Florianópolis/SC - CEP 88010-002
Ref.: Proposta Comercial da Licitação n. 1079455 **– Pregão Eletrônico n. 30/2025.**

LOTE 01						
Item	**Descritivo**	**Part Number**	**Unid.**	**Qtd.**	**Valor Unit. Item (R$)**	**Valor Total Item (R$)**
1	Firewall Fortigate 40F	FG-40F	Unid.	6		
2	Licença para Fortigate 40F - UTP	FC-10-0040F-950-02-60	Unid.	5		
3	Licença Forticare para Fortigate 40F	FC-10-0040F-314-02-60	Unid.	1		
4	Firewall Fortigate 60F	FC-60F	Unid.	9		
5	Licença para Fortigate 60F - UTP	FC-10-0060F-950-02-60	Unid.	8		
6	Licença Forticare para Fortigate 60F	FC-10-0060F-314-02-60	Unid.	1		
7	Firewall Fortigate 100F	FC-100F	Unid.	10		
8	Licença para Fortigate 100F - UTP	FC-10-F100F-950-02-60	Unid.	10		
9	Firewall Fortigate 120G	FC-120G	Unid.	6		
10	Licença para Fortigate 120G - UTP	FC-10-F120G-950-02-60	Unid.	5		
11	Licença Forticare para Fortigate 120G	FC-10-0120G-247-02-60	Unid.	1		
12	Licença FortiAnalyzer – Subscrição	FC1-10-AZVMS-465-01-60	Unid.	6		
13	Licença Forticare Premium Fortimanager 1-110	FC2-10-M3004-248-02-60	Unid.	1		
14	Licença Fortimanager Perpétua 10 Upgrade	FMG-VM-10-UG	Unid.	1		
15	Licença Coterm FG100FTK19000952 UTP	COTERM	Unid.	1		
16	Licença Coterm FG100FTK19000957 UTP	COTERM	Unid.	1		
17	Licença Coterm FG100FTK19000649 FORTICARE	COTERM	Unid.	1		
18	Serviços de instalação remota	-	Unid.	1		
19	Banco de Horas	-	Horas	300		
Valor Global da Proposta						

Valor Global do Lote para 5 (cinco) anos: R$ numérico e por extenso.

Validade da proposta: não inferior a 30 (trinta) dias.
Prazo para entrega e instalação remota: Até 30 (trinta) dias consecutivos contados a partir da assinatura física ou a partir do primeiro dia útil posterior a data da última assinatura eletrônica/digital do contrato.
Local de entrega: Rua Felipe Schmidt, 785, Sétimo Pavimento, Centro – Florianópolis/SC, CEP 88.010-002
Razão Social:
Endereço:
Fone:
E-mail:
Dados de quem irá assinar o Contrato:

Nome		Cargo	
e-mail		CPF	
Possui certificado digital	( ) Sim ( ) Não		

Dados Bancários:
Banco:
Agência:
Conta Corrente:

Este documento deverá estar datado, ser preenchido, conforme modelo, em papel timbrado da empresa licitante (dados para contato, e-mail, CNPJ, endereço) e estar devidamente assinado por seu representante legal.

PREGÃO ELETRÔNICO N. 30/2025

LICITAÇÃO N. 1079455

ANEXO IV –MINUTA DO CONTRATO

CONTRATAÇÃO DE EMPRESA PARA AQUISIÇÃO DE FIREWALLS E LICENÇAS DE FIREWLLS, QUE ENTRE SI CELEBRAM O SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – DEPARTAMENTO REGIONAL – SENAC/SC E A EMPRESA .....

CONTRATANTE: SENAC - Serviço Nacional de Aprendizagem Comercial – Administração Regional em Santa Catarina.
ENDEREÇO SEDE: Rua Felipe Schmidt, n. 785, 6º e 7º andares - Centro – CEP 88.010-002
CIDADE: Florianópolis/SC.
CNPJ: 03.603.739/0001-86
FONE: (48) 3251-0500
Representado neste ato pelo Presidente do Conselho Regional, Senhor Hélio Dagnoni, inscrito no CPF sob o n. [n. CPF], e pelo Diretor Regional do Senac/SC, Senhor Fabiano Battisti Archer, inscrito no CPF sob n. [n. CPF].

CONTRATADA:
ENDEREÇO SEDE:
CIDADE:
CNPJ:
FONE:
Representada neste ato por seu ___, Senhor___, inscrito no CPF sob o n. ___e RG sob o n. _____.

As partes acima identificadas e qualificadas, decidem firmar entre si o presente Contrato, segundo os termos e as condições seguintes.

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. Constitui objeto do presente Instrumento a aquisição de FIREWALLS E LICENÇAS de FIREWALLS, contemplando todos os softwares e suas licenças de uso, gerenciamento centralizado, garantia do fabricante, suporte técnico e treinamento, se

aplicável, de acordo com as especificações contidas no Pregão Eletrônico n. 30/2025, Termo de Referência e proposta de preço da **CONTRATADA**.
1.2. Integram o presente Contrato:

1.2.1. Edital de Pregão Eletrônico n. 30/2025.

1.2.2. Termo de Referência – **Anexo I** do Edital do Pregão Eletrônico n. 30/2025.

1.2.3. Proposta de preços da **CONTRATADA**, nº _____,de / /2025.

CLÁUSULA SEGUNDA - DA VIGÊNCIA, DA EXECUÇÃO, DA ENTREGA E INSTALAÇÃO

2.1. O prazo de vigência deste Contrato será de 60 (sessenta) meses ininterruptos, contados a partir de sua assinatura física ou a partir do primeiro dia útil posterior a data da última assinatura eletrônica ou digital, podendo ser prorrogado ao seu término, por igual e sucessivo período, até o limite previsto na Resolução Senac 1.270/2024, desde que as condições permaneçam vantajosas. Portanto, a **CONTRATADA** deverá cumprir com todas as atividades requeridas neste período, inclusive a garantia da Plataforma fornecida, e substituição dos mesmos, caso haja necessidade.
2.2. As Partes declaram que possuem capacidade jurídica para assinar eletronicamente ou digitalmente o presente instrumento, não podendo alegarem posteriormente a oposição de assinatura por quaisquer fatores que possam vir a entender como um impedimento. São os únicos responsáveis pelo sigilo e uso de seus e-mails, telefones celulares e senhas para consecução da assinatura eletrônica ou digital e que seu uso é pessoal e intransferível, devendo indenizar aqueles que sofrerem danos e/ou prejuízos pela utilização incorreta e/ou fraudulenta da assinatura eletrônica ou digital.

2.3. O prazo de execução deste Contrato será de 60 (sessenta) meses ininterruptos, portanto, a **CONTRATADA** disponibilizará a licença em conformidade com o Anexo I do Edital do Pregão Eletrônico n.30/2025, contados a partir de sua assinatura física ou a partir do primeiro dia útil posterior a data da última assinatura eletrônica ou digital.

2.4. O prazo para entrega dos equipamentos e conclusão da instalação remota será de até **30 (trinta) dias corridos**, contados a partir da assinatura física do contrato ou do primeiro dia útil subsequente à data da última assinatura eletrônica ou digital. A **CONTRATADA** deverá realizar a entrega dos equipamentos e executar a instalação remota em conformidade com as especificações técnicas constantes do **Anexo I** do Edital do Pregão Eletrônico nº 30/2025.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATADA:

3.1. Cumprir fielmente as obrigações assumidas em razão da assinatura do presente Contrato e do Anexo I, nos termos do Edital, proposta de preços, bem como pelas determinações e orientações que, durante o prazo contratual, lhe forem repassadas pelo **CONTRATANTE**.

3.1.1**.** Entregar o objeto acompanhado do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada, se aplicável.

3.1.2. Emitir relatórios técnicos periódicos e apresentar indicadores de desempenho sempre que solicitado pelo **CONTRATANTE**, observando o prazo previamente acordado entre as partes para sua elaboração e entrega.

3.2. Em nenhuma hipótese a **CONTRATADA** poderá alegar desconhecimento das Cláusulas, condições e especificações deste Contrato nem alegar qualquer erro involuntário ou omissão existente para eximir-se de suas responsabilidades.

3.3. Franquear e facilitar o **CONTRATANTE** ou preposto devidamente credenciado, a fiscalização do objeto deste Contrato, fornecendo, quando solicitados, todos os dados a ele relativos que sejam julgados necessários ao bom entendimento e acompanhamento do objeto contratual, sem que tal fiscalização implique em transferência de responsabilidade para o **CONTRATANTE** ou seu preposto.

3.4. Dar ciência imediata à fiscalização do **CONTRATANTE**, de toda e qualquer anormalidade que se verificar na execução dos serviços, sob pena de responsabilidade.

3.5. Arcar com despesas de deslocamento, alimentação e hospedagem dos profissionais alocados na execução dos serviços.

3.6. Responsabilizar-se por quaisquer processos ou ações, judiciais ou administrativas, bem como por todos os danos, pessoais ou materiais, diretos ou indiretos, que seus profissionais ou prepostos causem ao **CONTRATANTE** ou à terceiros, durante a execução do serviço, decorrente de ação ou omissão e decorrentes de culpa ou dolo, procedendo imediatamente aos reparos ou indenizações cabíveis e assumindo todos os ônus decorrentes.

3.7 Responsabilizar-se por todos os encargos de natureza trabalhista, social, previdenciária e/ou fiscal, relativos aos prepostos designados para realizar os serviços objetos deste Contrato, assumindo, em consequência, a condição de única empregadora, isentando o **CONTRATANTE**, inclusive judicialmente, de qualquer responsabilidade quanto a estes.

3.8. Responsabilizar-se integralmente pelos serviços contratados nos termos da legislação vigente, em conformidade com as especificações técnicas.

3.9. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições que culminaram em sua habilitação e qualificação na fase da licitação.

3.10. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

3.11. Responsabilizar-se pelos danos causados diretamente ao **CONTRATANTE** ou a terceiros decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo dessa responsabilidade a fiscalização do **CONTRATANTE** em seu acompanhamento.

3.12. Designar preposto para representar a **CONTRATADA** na execução do contrato.

3.13. Responsabilizar-se civil e criminalmente pelos danos causados ao **CONTRATANTE** ou a terceiros, decorrentes da execução do contrato.

3.14. Prestar os esclarecimentos desejados, bem como comunicar imediatamente ao **CONTRATANTE** quaisquer fatos ou anormalidades que, porventura, possam prejudicar o bom andamento ou o resultado final dos serviços.

3.15. Fornecer ao **CONTRATANTE** ou preposto seu, toda e qualquer informação que lhe seja solicitada sobre o objeto deste contrato, bem como facilitar-lhe a fiscalização da execução dos serviços contratados, cuja omissão na fiscalização, não diminui ou substitui a responsabilidade da **CONTRATADA**, decorrente das obrigações pactuadas;

3.16. Ficar ciente que não poderá utilizar o nome do **CONTRATANTE**, ou sua qualidade de **CONTRATADA** em quaisquer atividades de divulgação empresarial, como por exemplo, em cartões de visitas, anúncios diversos, impressos, folders, home page, etc., sob pena imediata rescisão do presente contrato, independente de aviso ou interpelação judicial ou extrajudicial, sem prejuízo das responsabilidades da **CONTRATADA**;

3.17. Assegurar ressarcimento dos bens do **CONTRATANTE** danificados de forma dolosa ou culposa, deduzindo o valor correspondente na nota fiscal/fatura da fatura do mês corrente;

3.18. Quaisquer erros, omissões ou irregularidades na elaboração dos serviços prestados serão de inteira responsabilidade da **CONTRATADA**, cabendo a ela sua imediata retificação, com base em notificação por escrito encaminhada pelo **CONTRATANTE**.

3.19. Manter sigilo sobre quaisquer informações do **CONTRATANTE** às quais tenha acesso.

3.20. Obedecer às demais condições previstas no Anexo I do Edital Pregão Eletrônico n. 30/2025, o qual constitui parte integrante deste instrumento.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE:

4.1. Fornecer à **CONTRATADA** e seus prepostos, tempestivamente, todas as informações e determinações que se fizerem necessárias à execução dos serviços contratados.

4.2. Notificar, por escrito, à **CONTRATADA**, fixando-lhe o prazo para correção de erros, defeitos ou irregularidades encontradas na execução do contrato, bem como sobre eventual aplicação de multa.

4.3. Prestar informações e esclarecimentos atinentes execução do contrato, que venham a ser solicitados pelos empregados da **CONTRATADA**.

4.4. Comunicar à **CONTRATADA** quaisquer falhas ocorridas, consideradas de natureza grave ou não, que tenham implicação, direta ou indireta, no cumprimento do objeto do presente Contrato.

4.5. Efetuar o pagamento relativo a aquisição dos equipamentos, banco de horas, nas condições previstas neste Contrato.

4.6. Indicar o gestor e/ou o fiscal para acompanhamento da execução contratual.

4.7. Exercer a fiscalização dos serviços por meio de colaboradores especialmente designados, verificando se, no desenvolvimento dos trabalhos, estão sendo cumpridos

serviços e especificações previstos no edital, no termo de referência, na proposta e no contrato de forma satisfatória, documentando as ocorrências.

4.8. Comunicar a falta de cumprimento das obrigações ao encarregado da **CONTRATADA** e, se necessário, ao supervisor da área, para que as falhas possam ser corrigidas a tempo.

4.9. Convocar a **CONTRATADA** para reuniões, sempre que necessário.

4.10. Manifestar-se formalmente em todos os atos relativos à execução do contrato.

4.11. Fornecer dados relativos as normas internas, diretrizes e informações necessárias para o fiel cumprimento do objeto contratual de acordo com as condições e peculiaridades do local;

CLÁUSULA QUINTA – DA EXECUÇÃO E GARANTIA:

5.1. O prazo de execução deste Contrato será de 60 (Sessenta) meses ininterruptos, podendo ser prorrogado ao seu término, por igual e sucessivo período, até o limite previsto na Resolução Senac 1.270/2024, mediante acordo entre as Partes, por intermédio de Termo Aditivo, desde que as condições permaneçam vantajosas. Portando, a **CONTRATADA** deverá entregar os equipamentos e instalações em conformidade com as condições e prazos, do Anexo I e III do Edital do Pregão Eletrônico n.30/2025, contados a partir de sua assinatura física ou a partir do primeiro dia útil posterior a data da última assinatura eletrônica/digital.

5.2. Caso o **CONTRATANTE** constate a existência de quaisquer irregularidades quanto ao objeto contratual, conforme estabelecido no Anexo I do Edital do Pregão Eletrônico n.30/2025, poderá recusar sua aceitação no momento da entrega e solicitar à **CONTRATADA** a substituição do item, no todo ou em parte, para que este seja adequado as exigências, dentro do prazo estipulado pelo **CONTRATANTE**, sem qualquer ônus adicional.

5.3. A **CONTRATADA** assegurará ao **CONTRATANTE** garantia dos serviços prestados pelo período de vigência contratual.

5.4. O descumprimento de quaisquer prazos dispostos nesta Cláusula, implicará nas sanções previstas na Cláusula Décima Segunda deste Contrato.

CLÁUSULA SEXTA – DO PAGAMENTO:

6.1. Pela aquisição dos equipamentos, licenças, e instalação, o **CONTRATANTE** pagará à **CONTRATADA**, em uma única parcela, o valor global de R$ (por extenso) em até 30 (trinta) dias subsequentes ao recebimento do objeto contratado, respeitando os dias de pagamento do SENAC/SC (dias 05, 15, 25 e 30 de cada mês), desde que tenham sido aceitos pelo SENAC/SC.

6.1.1. O pagamento das horas contratadas será efetuado conforme a demanda efetivamente utilizada, ou seja, o **CONTRATANTE** pagará à **CONTRATADA** somente pelas horas de suporte que forem efetivamente solicitadas e prestadas pela **CONTRATADA**, respeitando os valores unitários previamente definidos no contrato, em até 30 (trinta) dias subsequentes a prestação dos serviços, respeitando os dias de pagamento do SENAC/SC (dias 05, 15, 25 e 30 de cada mês), desde que tenham sido aceitos pelo SENAC/SC..

6.2. O(s) pagamento(s) será(ão) efetuado(s) mediante apresentação dos seguintes documentos/informações:

a) Nota fiscal (discriminando os serviços e seus valores, impostos e encargos);

b) Dados bancários completos para crédito em conta corrente, quando for o caso;

c) Indicação do número do contrato quando houver;

d) Mediante apresentação da prova de regularidade fiscal conforme item 4.3 e seus subitens do Edital de Licitação.

e) Prazo da garantia nas informações da Nota fiscal

6.3. Fica acordado que somente será de responsabilidade do **CONTRATANTE** o pagamento do objeto contratado no valor expresso no item 6.1 desta Cláusula, onde já estão embutidas todas as demais despesas decorrentes do deslocamento, alimentação, hospedagem do seu pessoal para entrega dos produtos, bem como quaisquer outras despesas como frete, seguro, impostos, e outros encargos que incidam ou venham incidir sobre o objeto ora contratado.

6.4. Havendo erro na apresentação da Nota Fiscal, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a **CONTRATADA** providencie as medidas saneadoras, iniciando-se o prazo para pagamento, estabelecido no item 6.1 acima, somente após a comprovação da regularização da situação, sem ônus para o **CONTRATANTE**.

6.4.1. Na hipótese de pagamento via crédito em conta corrente, é dever da **CONTRATADA** informar e manter atualizados os dados bancários, cabendo-lhe comunicar ao **CONTRATANTE**, de imediato, qualquer alteração.

6.4.2. Responsabilizar-se-á integralmente a **CONTRATADA** por pagamento indevido em razão da falta, erro de informação ou de atualização dos dados bancários.

6.4.3. Se a **CONTRATADA** for usuária da NF-e, ao emitir nota fiscal para o SENAC/SC enviar o arquivo XML da mesma para o e-mail: notas.compras@sc.senac.br.

6.5. O faturamento e a cobrança será efetuado através da emissão de nota fiscal para o **CONTRATANTE**, conforme abaixo:

Nome:	**SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL - SENAC**
CNPJ:	03.603.739/0001-86
Insc. Est.:	Isento
Endereço:	Rua Felipe Schmidt, 785, 6 e 7 andar – Centro – Florianópolis/SC- CEP 88.010-002

6.6. A nota fiscal deverá ser emitida nos termos e limites da legislação tributária vigente nas esferas federal, estadual e municipal, já constando todos os tributos incidentes, a descrição do objeto contratado e o mês de referência.

6.7. A **CONTRATADA** deverá anexar na nota fiscal, sempre que solicitado pelo **CONTRATANTE**, fotocópia dos documentos que comprovem sua regularidade fiscal, tais como:

6.7.1. Prova de regularidade para com a Fazenda Nacional, composta da Certidão Conjunta expedida pela Secretaria da Receita Federal do Brasil e pela Procuradoria Geral da Fazenda Nacional, referente a todos os créditos tributários federais e à Dívida Ativa da União, abrangendo, ainda, as contribuições previstas nas alíneas "a", "b" e "c" do parágrafo único do art. 11 da Lei n. 8.212, de 24/07/1991, conforme Portaria Conjunta RFB/PGFN nº 1.751 de 02/10/2014.

6.7.2. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), composta da Certidão de Regularidade Fiscal (CRF) ou outro meio equivalente, no cumprimento dos encargos instituídos por lei.

6.8. É vedado à **CONTRATADA** negociar os títulos de crédito emitidos contra o **CONTRATANTE**, bem como a antecipação de pagamento de qualquer natureza.

6.9. Quando do pagamento da fatura, serão deduzidos valores referentes aos tributos e contribuições federais, estaduais e municipais incidentes, conforme legislação vigente.

CLÁUSULA SÉTIMA – DO REAJUSTE:

7.1. O presente contrato é irreajustável pelo prazo de 60 (sessenta) meses. A partir do 61° mês, aplicar-se-á o IPCA, acumulado nos últimos 12 (doze) meses, em caso de renovação, desde que as condições permaneçam vantajosas, nos moldes do art. 33 da Resolução 1.270/2024.

CLÁUSULA OITAVA – DA FISCALIZAÇÃO:

8.1. A execução do objeto deste Contrato será fiscalizada pelo **CONTRATANTE**, por sua Diretoria Administrativa, por intermédio do Setor de Tecnologia da Informação e Comunicação da Administração Regional do Senac/SC que poderá fornecer à **CONTRATADA** orientação quanto à execução e qualidade exigidas na execução contratual.

8.1.1.1. Exigir da **CONTRATADA** a estrita observância às estipulações deste Contrato, à documentação a ele anexa, às normas do **CONTRATANTE**.

8.1.1.2. Determinar os prazos para cumprir as exigências feitas.

8.2. A cada vez que a fiscalização do **CONTRATANTE** notificar o aviso de um defeito e o respectivo prazo de correção, começará o período de correção de defeito para o que a **CONTRATADA** foi informada. A mesma deverá corrigi-lo no prazo definido pelo **CONTRATANTE**. A **CONTRATADA** tem a responsabilidade de correção dos defeitos que ela própria identifique antes do fim do prazo de observação. O **CONTRATANTE** deverá certificar que todos os defeitos foram corrigidos.

8.3. A fiscalização exercida pelo **CONTRATANTE** não excluirá, nem reduzirá, a responsabilidade da **CONTRATADA** por controle, fiscalização, execução do objeto contratual e qualquer irregularidade, inclusive perante terceiros.

CLÁUSULA NONA – DA SUBCONTRATAÇÃO:

9.1. O **CONTRATANTE** não aceitará, em nenhuma hipótese, subcontratação para o objeto deste Contrato.

CLÁUSULA DÉCIMA – DAS ALTERAÇÕES:

10.1. Nenhuma das disposições deste Contrato poderá ser considerada renunciada ou alterada, salvo se for especificamente formalizada por meio de Termo Aditivo. O fato de uma das partes tolerar qualquer falta ou descumprimento de obrigações da outra, não importa em alteração do Contrato e nem induz à novação, ficando mantido o direito de se exigir da parte faltosa ou inadimplente, a qualquer tempo, a cessão da falta ou o cumprimento integral da tal obrigação.

10.2. A **CONTRATADA** fica obrigada a acatar, nas mesmas condições deste Contrato, por ato unilateral do **CONTRATANTE**, os acréscimos que se fizerem necessários, até o limite de 50% (cinquenta por cento) do valor inicial atualizado, conforme estipulado no artigo 38 da Resolução Senac n° 1.270/2024.

10.3. As supressões poderão ser realizadas nos limites convencionados entre as partes.

CLÁUSULA DÉCIMA PRIMEIRA – DA NOVAÇÃO:

11.1. A não utilização, pelo **CONTRATANTE**, de qualquer direito a ela assegurado neste Contrato ou na Lei em geral, ou a não aplicação de quaisquer das sanções nele previstas, não importará em novações quanto a seus termos, não devendo, portanto, ser interpretada como renúncia ou desistência de aplicação ou de ações futuras.

CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO E DAS PENALIDADES:

12.1. As sanções administrativas para os casos de descumprimento das cláusulas, inexecução total ou parcial das obrigações assumidas e demais condições estabelecidas no presente instrumento, excluídas as hipóteses de caso fortuito ou força maior, desde que devidamente comprovadas, serão, inclusive cumulativamente, aplicadas: **advertência, multa, suspensão temporária do direito de licitar ou de contratar com o Senac por prazo não superior a 3 (três) anos e impedimento do direito de licitar, com abrangência nacional por, no mínimo 04 (quatro) e, no máximo 06 (seis) anos.**

12.2. A sanção de **advertência** será efetuada por escrito, comunicando de forma objetiva, qual item do contrato ou Termo de Referência deixou de ser cumprido, e cobrando providências. Esse tipo de sanção corresponde a ato praticado pela **CONTRATADA** que não seja suficiente para acarretar prejuízo ao **CONTRATANTE**, suas instalações, pessoas, imagem, meio ambiente, ou a terceiros. que venham ou não causar danos ao **CONTRATANTE** ou a terceiros.

12.3**.** A **CONTRATADA** estará sujeita às seguintes MULTAS:

12.3.1. Multa moratória de 1% (um por cento) do valor do objeto em atraso, por dia de atraso, limitada a 30% (trinta por cento) do valor do objeto em atraso.

12.3.2. Multa Compensatória de até 15% (quinze por cento) da parcela inadimplida em caso de inadimplemento parcial ou total, sem prejuízo da apuração das perdas e danos, que deverão ser demonstradas e comprovadas.

12.3.3. As multas serão cobradas, a critério do **CONTRATANTE**, por uma das formas a seguir enumeradas:

12.3.3.1. Mediante desconto no recebimento a que a **CONTRATADA** tiver direito;

12.3.3.2**.** Mediante cobrança extrajudicial e/ou judicial;

12.4. Suspensão do direito de licitar ou contratar com o Senac.

12.4.1. Suspensão temporária de participação em processos de licitação e impedimento de contratar com as Unidades integrantes do Senac/SC, pelo prazo não superior a 03 (três) anos, conforme Artigo 39, inciso III, da Resolução SENAC n. 1.270/2024, em vigor a partir de 2 de maio de 2024;

12.4.2 As hipóteses previstas nos itens I, II, III e IV abaixo ensejarão impedimento do direito de licitar e terão abrangência nacional, por prazo mínimo de 4 (quatro) e máximo de 6 (seis) anos:

I. Apresentar declaração ou documentação falsa exigida durante a execução deste Contrato;

II. Praticar ato fraudulento na execução do presente Contrato;

III. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

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

12.5. Rescisão e Resolução do contrato.

12.5.1. O **CONTRATANTE** poderá rescindir o presente contrato, sem que assista à **CONTRATADA** qualquer direito de indenização, nos seguintes casos:

12.5.1.1. Não cumprimento ou cumprimento irregular de cláusulas contratuais, especificações, projetos ou prazos, sem prejuízo da aplicação das demais penalidades previstas;

12.5.1.2. Não proceder às retificações ou determinações do **CONTRATANTE**, realizadas por escrito e no prazo indicado;

12.5.1.3. Transferir o contrato a terceiros sem a expressa anuência do **CONTRATANTE**;

12.5.1.4. Perder qualquer condição de habilitação exigida no processo de licitação;

12.5.1.5. Decretação de falência, a instauração de insolvência ou ainda a dissolução da **CONTRATADA**;

12.5.1.6. Ocorrência de caso fortuito ou força maior, regularmente comprovada, impeditiva da execução do contrato;

12.5.1.7. Superveniente incapacidade técnica ou financeira, devidamente comprovada;

12.5.1.8. Suspensão dos serviços por determinação de autoridades, motivado pela **CONTRATADA**, a qual responderá por perdas e danos que o **CONTRATANTE**, como consequência, venha a sofrer.

12.5.1.9. Ocorrer reincidência, por parte da **CONTRATADA**, em infração contratual que implique na aplicação de multa.

12.5.2. Por acordo entre as partes, desde que haja conveniência ao **CONTRATANTE**.

12.5.3. Judicialmente, nos termos da legislação vigente.

12.5.4. Se ocorrer a hipótese da resolução por parte do **CONTRATANTE**, caberá à **CONTRATADA** o direito ao recebimento das faturas correspondentes aos serviços que tiverem sido prestados e aceitos, sendo que o interesse em rescindir este contrato deverá ser formalizado por intermédio de ofício, com antecedência mínima de 30 (trinta) dias.

12.5.5. Caso a **CONTRATADA** possua outros contratos firmados com o SENAC/SC, estes também serão rescindidos visto à aplicação da sanção do item 12.4.1. e 12.4.2.

12.5.6. Além de qualquer outro descumprimento de cláusula contratual constituem causa de resolução, em qualquer tempo, independentemente de interpelação judicial ou extrajudicial, sem que a **CONTRATADA** tenha direito a indenização, a qualquer título:

12.5.6.1. Ceder ou transferir, no todo ou em parte, os direitos e serviços que constituem objeto do Contrato, sem a prévia autorização.

12.5.6.2. Deixar de cumprir as obrigações previstas no contrato e na legislação trabalhista.

12.5.6.3. Ocorrer reincidência, por parte da **CONTRATADA**, em infração contratual que implique na aplicação de multa.

12.5.6.4. Ocorrer a decretação de falência, a liquidação judicial ou extrajudicial da **CONTRATADA**, ou ainda, o ingresso desta última em processo de recuperação judicial.

12.5.6.5. Em qualquer das situações elencadas nos itens acima, exceto o previsto no item 7.10.4, a **CONTRATADA** ficará sujeita à multa resolutória equivalente a 5% (cinco por cento) do valor estimado da contratação, cumulativamente, respondendo ainda, pelas perdas e danos decorrentes.

12.5.6.6. Se ocorrer à hipótese da resolução por parte do **CONTRATANTE**, caberá à **CONTRATADA** o direito ao recebimento das faturas correspondentes aos serviços que tiverem sido prestados e aceitos.

12.6. A **CONTRATADA** não será responsabilizada por atrasos resultantes de casos fortuitos ou de força maior, desde que esses fatos sejam devidamente comprovados e tenham influência direta no atraso verificado.

12.7. A **CONTRATADA** deverá comunicar, por escrito e justificadamente, as ocorrências de caso fortuito ou força maior impeditivas da prestação dos serviços, no prazo máximo de 2 (dois) dias úteis contados da data da ocorrência, sob pena de não poder alegá-los posteriormente.

12.8. Não serão aceitas como justificativas de atraso da **CONTRATADA** as alegações de atraso por parte de seus eventuais fornecedores, exceto quando resultantes de caso fortuito ou força maior.

12.9. As penalidades descritas são independentes, podendo ser aplicadas isolada ou cumulativamente, dependendo apenas da ocorrência dos fatos geradores. Não incidirão, todavia, sobre as infrações decorrentes de "caso fortuito" ou de "força maior", desde que devidamente justificadas e comprovadas.

12.10. As multas poderão ser aplicadas tantas vezes quantas forem às irregularidades constatadas.

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO:

13.1. O presente Contrato poderá ser extinto nas seguintes hipóteses:

13.1.1. Resilição a qualquer tempo, por quaisquer das partes, mediante comunicação por escrito, com antecedência mínima de 30 (trinta) dias corridos da data em que se pretender extingui-lo, momento em que deverão ser observadas as obrigações contraídas no período.

13.1.2. Por descumprimento de quaisquer das Cláusulas, independente de ações legais.

13.1.3. Em caso de dissolução ou liquidação societária insolvência ou em caso de falecimento quando se tratar de Sociedade Limitada Unipessoal (SLU).

13.1.4. Quando, justificadamente, não for mais do interesse do **CONTRATANTE**.

13.1.5. Atraso injustificado para conclusão do serviço por mais de 10 (dez) dias consecutivos ou ensejar retardamento da execução do objeto.

13.1.6. Superveniente incapacidade técnica da **CONTRATADA**, devidamente comprovada.

13.1.7. Negar-se a **CONTRATADA** a refazer qualquer trabalho realizado em desacordo com as especificações técnicas constantes deste Contrato e do Anexo I do Edital Pregão Eletrônico n. 30/2025, no prazo que, para tanto determinar a fiscalização do **CONTRATANTE**.

CLÁUSULA DÉCIMA QUARTA – DA CONFIDENCIALIDADE:

14.1. A **CONTRATADA** se compromete a manter sigilo e confidencialidade sobre todas e quaisquer informações verbais ou escritas, cedidas ou reveladas por ocasião do presente Contrato, responsabilizando-se pela reparação de danos em caso de violação da obrigação ora assumida.

14.2. A **CONTRATADA** obriga-se a não usar ou revelar qualquer informação acerca da execução do presente Contrato, a terceiros, para quaisquer fins, sem o acordo prévio do **CONTRATANTE**. Esta obrigação subsistirá pelo período de vigência deste Contrato, bem como pelo período de 5 (cinco) anos contados da data do término ou da rescisão do presente Contrato.

CLÁUSULA DÉCIMA QUINTA – DA LGPD:

15.1. O **CONTRATANTE** tem compromisso com a privacidade e a proteção de dados pessoais de seus colaboradores, clientes e parceiros. E, nesse sentido, envida seus melhores esforços para, no tratamento de dados pessoais decorrente deste contrato, observar integralmente a legislação aplicável, em especial a Lei nº 13.709/2018 (LGPD). Da mesma forma a **CONTRATADA** deve observar integralmente o disposto na legislação supracitada, sob as penas da lei.

Parágrafo único – É vedado a utilização de todo e qualquer dado pessoal repassado em decorrência deste instrumento para finalidade distinta daquela do objeto desta parceria, sob pena de responsabilização administrativa, civil e criminal, conforme Lei nº 13.709/2018.

CLÁUSULA DÉCIMA SEXTA – DOS RECURSOS ORÇAMENTÁRIOS:

16.1. As despesas decorrentes deste Contrato correrão por conta do Centro de Custo 900005003 - Padronização de Firewall Senac/SC, conforme Requisições 234972 e 234965, e Processo n. 13073.

CLÁUSULA DÉCIMA SÉTIMA – DAS DISPOSIÇÕES FINAIS:

17.1. Todas as comunicações e notificações relativas ao presente Contrato serão consideradas como regularmente feitas pelo **CONTRATANTE**, se entregues ou enviadas por carta protocolizada ou *e-mail* para o endereço da **CONTRATADA**.

17.2. A **CONTRATADA** declara ter ciência e se compromete a cumprir os princípios e regras contidos no Código de Ética do **CONTRATANTE**, disposto no *site*: https://transparencia.senac.br/#/sc/controle-interno-externo

17.3. A **CONTRATADA** declara ter ciência e se compromete a cumprir os princípios e regras contidos na Política de Conduta para Fornecedor/Prestador de serviços do Senac/SC POLÍTICA DE CONDUTA, disposto no site: https://portal.sc.senac.br/doc/area-do-fornecedor/politica-de-conduta-fornecedores-servicos-senac.pdf

17.4. Qualquer mudança de endereço, denominação, de tipo societário ou alteração relativa à reorganização societária da **CONTRATADA** deverá ser imediatamente comunicada à **CONTRATANTE.**

17.5. Os prazos estipulados neste Contrato, para cumprimento das obrigações contratuais, vencem independentemente de interpelação judicial ou extrajudicial.

17.6. Se alguma Cláusula ou condição deste Contrato for total ou parcialmente anulada judicialmente, tal nulidade afetará unicamente a disposição contratual pertinente, vinculando às partes ao restante deste Contrato, como se a disposição nula não o integrasse.

17.7. É vedado à **CONTRATADA** utilizar-se de marcas, logotipos ou expressões de propaganda do **CONTRATANTE**, a não ser mediante autorização desta por escrito.

17.8. Admitir-se-á a continuidade deste Contrato na hipótese de a **CONTRATADA** passar por operações de reorganização societária, tais como cessão ou transferência total ou parcial, transformação, fusão, cisão e incorporação, desde que sejam observados pela nova empresa os requisitos de habilitação previstos no Edital e em conformidade com a Resolução Senac 1.270/2024, e ainda, que sejam mantidas as condições inicialmente estabelecidas.

17.9. As partes convencionam que eventuais diferenças poderão ser compensadas ou deduzidas mediante prévia e expressa solicitação da parte interessada e consentimento da parte contrária.

CLÁUSULA DÉCIMA OITAVA – DA POLÍTICA ANTICORRUPÇÃO:

18.1. Pelo presente instrumento contratual, a **CONTRATADA** se compromete a observar as normais legais vigentes no país, incluindo, mas não se limitando, à Lei Anticorrupção (Lei nº 12.846/2013) e à Lei contra a Lavagem de Dinheiro (Lei nº 9.613/1998), bem como se obriga a agir em consonância às políticas internas do **CONTRATANTE**.

18.2. A **CONTRATADA** declara, por livre manifestação, não estar envolvida, direta ou indiretamente, por meio de seus representantes, administradores, diretores, sócios, consultores ou partes relacionadas, em qualquer atividade ou prática que caracterize infração administrativa nos termos da Lei Anticorrupção.

18.3**.** A **CONTRATADA** declara que, direta ou indiretamente, não forneceu, pagou ou autorizou o pagamento, nem concordou em dar presentes ou qualquer objeto de valor a qualquer pessoa ou entidade, pública ou privada, com o objetivo de beneficiar-se ou beneficiar o **CONTRATANTE** ilicitamente e se compromete a não fazê-lo durante toda a vigência do presente contrato.

18.4. As partes se comprometem a não contratarem como empregados ou firmarem qualquer forma de relacionamento profissional com pessoas físicas ou jurídicas envolvidas em atividades criminosas, em especial pessoas investigadas pelos delitos previstos nas leis anticorrupção e de lavagem de dinheiro.

18.5. A **CONTRATADA** se obriga a notificar o **CONTRATANTE**, imediatamente, por escrito, a respeito de qualquer suspeita ou violação das legislações vigentes, bem como em casos em que obtiver ciência acerca de qualquer prática de suborno ou corrupção.

18.6. O descumprimento pela **CONTRATADA** das normas legais anticorrupção e do disposto neste Contrato será considerado uma infração grave e implicará na possibilidade de rescisão do instrumento contratual pelo **CONTRATANTE**, sem qualquer ônus ou penalidade, respondendo a **CONTRATADA**, ainda, sobre eventuais perdas e danos.

CLÁUSULA DÉCIMA NONA –FORO:

19.1. As partes elegem o foro da Comarca da cidade de Florianópolis/SC, para resolver ou dirimir qualquer ação ou execução decorrente deste Contrato, renunciando a qualquer outro, por mais privilegiado que seja.

Por estarem justas e de comum acordo, as partes assinam o presente Contrato em 2 (duas) vias, de igual teor, e para um só efeito, na presença das testemunhas abaixo assinadas.

(se for assinatura digital/eletrônica)

E por estarem justos e contratados, assinam o presente instrumento contratual, dispensando-se a assinatura das testemunhas conforme §4° do artigo 784 do Código de Processo Civil.

Hélio Dagnoni
Presidente do Conselho Regional do SENAC/SC

Fabiano Battisti Archer
Diretor Regional do SENAC/SC

CONTRATADA
Representante legal da empresa

Testemunha do **CONTRATANTE**

1 -
Nome:
CPF:

Testemunha da **CONTRATADA**

2 -
Nome:
CPF:

ANEXO I DO CONTRATO

(Este anexo será composto da proposta de preços da licitante vencedora e Termo de Referência)