**PREGÃO ELETRÔNICO – PEE 2025000116**

O **Serviço Nacional de Aprendizagem Comercial – Senac**, Administração Regional no Estado de São Paulo ("**Senac**"), torna pública a realização de **LICITAÇÃO**, na modalidade **PREGÃO na forma eletrônica** ("**Pregão**"), nos termos do presente Edital e seus Anexos.

**RESUMO DA LICITAÇÃO**

**OBJETO: "AQUISIÇÃO DAS SOLUÇÕES TREND MICRO PARA SEGURANÇA DA INFORMAÇÃO DAS ESTAÇÕES DE TRABALHO E SERVIDORES, COM GESTÃO CENTRALIZADA E PROTEÇÃO PARA CARGAS DE TRABALHO HÍBRIDAS. INCLUI GERENCIAMENTO DE RISCO CIBERNÉTICO, IDENTIFICAÇÃO DE EXPOSIÇÃO EXTERNA E DETECÇÃO E RESPOSTA ESTENDIDA PARA ATENDER O SENAC SÃO PAULO E DRS PARTICIPANTES".**

**RECEBIMENTO DA PROPOSTA ELETRÔNICA NO PORTAL DE COMPRAS E CONTRATAÇÕES DO SENAC SÃO PAULO:**
De 05/12/2025 até às 09h45 do dia 15/12/2025.

**ABERTURA DAS PROPOSTAS ELETRÔNICAS:**
A partir das 10h00 do dia 15/12/2025.

**INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS:**
Às 10h00 do dia 15/12/2025.

**DISPONIBILIDADE DO EDITAL:**
**PORTAL DE COMPRAS E CONTRATAÇÕES DO SENAC SÃO PAULO,** no *site* https://egov.paradigmabs.com.br/senacsp e na Sede da Administração Regional do **Senac São Paulo**, localizada na Rua Dr. Vila Nova, 228, 7º andar – Sala 705, Vila Buarque, São Paulo/SP, CEP:01222-020.

**PEDIDOS E RESPOSTAS DE ESCLARECIMENTOS:**
Os interessados poderão encaminhar solicitação de esclarecimentos, até o dia **11 de dezembro de 2025**, por meio do Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, na aba "Mural", no campo "**ESCLARECIMENTOS**", em relação a eventuais dúvidas de interpretação do presente Edital e seus Anexos, visando à sua melhoria. As questões formuladas serão respondidas, por escrito, a todos os interessados, até o dia **12 de dezembro de 2025**. Não serão fornecidos esclarecimentos verbais por funcionários do Senac em quaisquer fases da presente licitação.
Não serão reconhecidas dúvidas encaminhadas por outro meio que não seja o Portal de Compras e Contratações do Senac São Paulo.

**Gerência de Materiais e Serviços**
**Senac São Paulo**

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
E-mail: licitacao.gms@sp.senac.br
www.sp.senac.br

**PREGÃO ELETRÔNICO – PEE 2025000116**

## 1. FUNDAMENTAÇÃO JURÍDICA

1.1. A presente licitação reger-se-á pelas normas e procedimentos do Regulamento de Licitações e Contratos do Senac, Administração Regional no Estado de São Paulo vigente (Resolução nº 18/2024), que pode ser consultado e/ou obtido por meio do link https://www1.sp.senac.br/hotsites/sites/licitacao/wp-content/uploads/2024/06/resoluc%CC%A7a%CC%83o-182024-regulamento-de-licitac%CC%A7o%CC%83es-e-contratos-do-senac-sp.pdf, e pelo presente Edital.

1.2. A contratação decorrente do presente processo licitatório se fará, no que lhe for aplicável, de acordo com o Termo Geral de Contratação do Senac São Paulo ("TGC"), devidamente registrado no 8º Oficial de Registro de Títulos e Documentos e Civil de Pessoa Jurídica da Comarca de São Paulo sob nº 1.591.854, que pode ser consultado e/ou obtido por meio do link https://www1.sp.senac.br/hotsites/sites/licitacao/wp-content/uploads/2025/03/termo-geral-de-contratacao-do-senac-sao-paulo-8-rtdpj-n-1591854-de-28022025.pdf.

## 2. OBJETO

2.1. A presente licitação destina-se a futura ou eventual **AQUISIÇÃO DAS SOLUÇÕES TREND MICRO PARA SEGURANÇA DA INFORMAÇÃO DAS ESTAÇÕES DE TRABALHO E SERVIDORES, COM GESTÃO CENTRALIZADA E PROTEÇÃO PARA CARGAS DE TRABALHO HÍBRIDAS. INCLUI GERENCIAMENTO DE RISCO CIBERNÉTICO, IDENTIFICAÇÃO DE EXPOSIÇÃO EXTERNA E DETECÇÃO E RESPOSTA ESTENDIDA PARA ATENDER O SENAC SÃO PAULO E DRS PARTICIPANTES**, conforme especificações e de acordo com as condições, quantidades e exigências descritas neste Edital.

## 3. CONDIÇÕES GERAIS PARA PARTICIPAÇÃO

3.1. Respeitadas as demais condições legais e as constantes deste Edital, poderão participar deste Pregão, como também firmar o contrato ou instrumento equivalente dele decorrente com o Senac, pessoas jurídicas que satisfizerem plenamente todos os termos e condições estabelecidas no Edital e seus anexos.

3.2. 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, procurador devidamente credenciado, ou seja, com poderes outorgados por meio de procuração, instrumento público ou particular, para representar a Licitante em processos licitatórios.

3.2.1. Somente poderão participar desta licitação as empresas **cujo ramo de atividade seja compatível com o objeto do presente Pregão**.

3.2.2. A participação na presente Licitação implica na aceitação integral e incondicional de todos os termos e condições constantes neste Edital e todos os seus anexos.

3.2.3. É vedado a qualquer pessoa física ou jurídica representar mais de uma Licitante na presente licitação.

3.3. **Não poderão participar do presente Pregão as empresas:**

a) Suspensas de licitar ou contratar com o Senac;
b) Em processo de falência, em recuperação judicial ou extrajudicial, em dissolução ou liquidação;
c) Consorciadas;
d) Que tenham em sua composição societária participação comum;
e) Que detenham um mesmo representante em comum.

3.3.1. A participação de empresas que estejam em recuperação judicial somente será permitida se amparada em certidão emitida pela instância judicial competente, que certifique que a interessada está apta econômica e financeiramente a participar de procedimento licitatório e desde que observadas as demais condições de habilitação.

3.4. Será **excluída sumariamente da licitação** a Licitante que estiver incursa em qualquer uma das vedações acima dispostas, **não cabendo interposição de recurso.**

3.5. A Licitante declara que leu e concorda com todos os termos do Código de Ética e Conduta Profissional do Senac São Paulo, disponível no http://sisnormas.sp.senac.br/sisnormas/downloads/codigo_de_etica_e_conduta_profissional_do_senac, e compromete-se a observá-lo e a cumpri-lo integralmente.

**4. DO ACESSO AO PORTAL DE COMPRAS E CONTRATAÇÕES DO SENAC SÃO PAULO**

4.1. Para participar do presente Pregão Eletrônico, os interessados deverão acessar o Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, para realizar o seu registro ou atualização cadastral, sendo, no mínimo, tipo **Básico**, com login e senha de acesso.

4.1.1. Para participação, o registro e/ou atualização cadastral, a homologação do cadastro pelo Senac, o credenciamento dos representantes que atuarão em nome da Licitante no Portal de Compras e Contratações do Senac São Paulo, bem como a obtenção de senha de acesso, deverão ser feitos **ANTERIORMENTE** à data de abertura da sessão pública.

4.1.2. O cadastro do interessado junto ao Sistema Eletrônico implica a responsabilidade legal pelos atos praticados e presunção de sua capacidade técnica e jurídica para realização das transações inerentes ao Pregão Eletrônico.

4.1.3. 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, qualquer responsabilidade por eventuais danos decorrentes de uso indevido de senha, ainda que por terceiros.

## 5. CONEXÃO COM O SISTEMA

5.1. Caberá à Licitante permanecer conectada ao Sistema Eletrônico para o acompanhamento das operações durante a sessão do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Sistema Eletrônico ou de sua desconexão.

5.2. 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.

5.3. A desconexão do Sistema Eletrônico com o Pregoeiro, durante a sessão, implicará as seguintes questões:

5.3.1. Fora da etapa de lances, a sua suspensão e o seu reinício, desde o ponto em que a sessão foi interrompida. Neste caso, se a desconexão persistir por tempo superior a 15 (quinze) minutos, a sessão será suspensa e retomada somente após comunicação expressa às Licitantes de nova data e horário para a sua continuidade;

5.3.2. Ocorrendo a desconexão com o Pregoeiro no decorrer da etapa de lances, mas o Sistema Eletrônico permanecer acessível às Licitantes, os lances continuarão sendo recebidos sem prejuízo dos atos realizados;

5.3.3. Quando a desconexão citada no **subitem 5.3.2** persistir por tempo **superior a 10 (dez) minutos**, a sessão poderá ser suspensa e retomada somente após a comunicação expressa do Pregoeiro às Licitantes.

5.4. A desconexão do Sistema Eletrônico com qualquer Licitante não prejudicará a conclusão válida da sessão ou da licitação.

## 6. HABILITAÇÃO

### 6.1. HABILITAÇÃO JURÍDICA

6.1.1. Ato constitutivo da sociedade, em conformidade com a legislação vigente (**Estatuto, Contrato Social ou outro pertinente à constituição da empresa**), acompanhado de todas as suas alterações, quando houver, ou a última alteração consolidada, devidamente registradas, acompanhadas, quando aplicável, dos respectivos documentos de eleição de seus administradores;

6.1.2. **Prova de registro**, no órgão competente, no caso de empresário individual;

6.1.3. **Ato de nomeações** ou de **eleição dos administradores**, devidamente registrados no órgão competente, nas hipóteses de terem sido nomeados ou eleitos em separado, sem prejuízo da apresentação dos demais documentos exigidos no **subitem 6.1.1**;

6.1.4. **Decreto de autorização**, em se tratando de empresa ou sociedade estrangeira em funcionamento no país, bem como ato de registro ou autorização para funcionamento expedido pelo órgão competente quando a atividade assim o exigir.

6.2. **REGULARIDADE FISCAL:**

6.2.1. Prova de inscrição atualizada no **Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda – CNPJ**, com situação ativa, relativa à sede da Licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

6.2.2. Prova de regularidade para com as fazendas federal, estadual e municipal do domicílio ou sede da Licitante, **na forma da lei**, por meio dos seguintes documentos:

6.2.2.1. Certidão Negativa ou Positiva com efeitos de Negativa de Débitos relativa aos **Tributos Federais** e Dívida Ativa da União, previstas nas **alíneas "a"** a **"d"** do parágrafo único do artigo 11 da Lei 8.212 de 24 de julho de 1991, expedida pela Secretaria da Receita Federal do Brasil ou Procuradoria Geral da Fazenda Nacional, nos termos da Portaria MF 358 de 05/09/2014;

6.2.2.2. Certidão Negativa ou Positiva com efeitos de Negativa de Débitos relativa aos **Tributos Estaduais** com referência especificamente ao ICMS – Imposto Sobre Circulação de Mercadorias e Serviços, expedida pela Fazenda Estadual, da sede da Licitante;

6.2.2.2.1. Em se tratando de sede no Estado de São Paulo, será aceita tanto a Certidão Negativa de Débitos Tributários da Dívida Ativa do Estado de São Paulo – CRDA, expedida pela Procuradoria Geral do Estado, quanto a Certidão Negativa de Débitos Tributários Não Inscritos na Dívida Ativa do Estado de São Paulo, expedida pela Secretaria da Fazenda do Estado de São Paulo;

6.2.2.3. Certidão Negativa ou Positiva com efeitos de Negativa de Débitos relativa aos **Tributos Municipais Mobiliários** com referência especificamente ao ISS – Imposto Sobre Serviços, expedida pela Secretaria da Fazenda Municipal;

6.2.3. **Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – CRF-FGTS** relativo à sede da Licitante, expedida pela Caixa Econômica Federal.

6.3. **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

6.3.1. **Certidão Negativa de Falência, Concordata e Recuperação Judicial e Extrajudicial**, expedida pelo Distribuidor Cível da Matriz da Licitante, com validade na data de abertura da presente Licitação.

6.4. **CONSIDERAÇÕES GERAIS SOBRE OS DOCUMENTOS**

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

6.4.2. Para dirimir dúvidas suscitadas no exame dos documentos de habilitação e/ou da proposta comercial, a Comissão Permanente de Licitação, em qualquer fase da licitação, poderá, a seu critério exclusivo, realizar diligências junto às Licitantes e/ou terceiros solicitando esclarecimentos e/ou comprovação a respeito da veracidade de informações e/ou dos documentos apresentados.

6.4.3. A Comissão Permanente de Licitação poderá, ainda, a seu critério, solicitar que qualquer Licitante supra ou saneie eventuais omissões ou falhas relativas no cumprimento dos requisitos e condições estabelecidos neste Edital, mediante a apresentação de documentos desde que os envie no curso da própria sessão **no prazo previamente estipulado**.

6.4.4. Com o objetivo de dirimir dúvidas suscitadas no exame dos documentos de habilitação e/ou da proposta comercial e/ou sanear eventuais omissões ou falhas relativas no cumprimento dos requisitos e condições estabelecidos neste Edital, o Senac poderá consultar o seu Cadastro de Fornecedores.

6.4.5. Todas as certidões elencadas acima, após solicitadas pelo Pregoeiro, deverão **estar válidas na data da sua apresentação**. A validade corresponderá ao prazo fixado nas próprias certidões, quando houver. Caso estas não contenham expressamente o prazo de validade, o Senac convenciona o prazo de **90 (noventa) dias corridos**, a contar da data de sua expedição, ressalvada a hipótese de a licitante comprovar que o documento tem prazo de validade inferior ou superior ao antes convencionado, mediante juntada de norma legal pertinente.

6.4.6. 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 quando ocorrido durante o certame.

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

6.4.8. 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 pela 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.

6.4.9. 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.

## 7. PROCEDIMENTOS LICITATÓRIOS

### 7.1. INÍCIO PARA CADASTRAMENTO E RECEBIMENTO DAS PROPOSTAS ELETRÔNICAS

7.1.1. O início para cadastramento das propostas se dará a partir do dia **05 de dezembro de 2025**.

7.1.2. A Licitante deverá preencher sua proposta exclusivamente no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, em conformidade com as exigências deste Edital.

7.1.3. Até às **09h45 o dia 15/12/2025**, os interessados poderão inserir ou substituir propostas de preços no sistema eletrônico. Após a abertura das propostas, não será admitido o envio/substituição de propostas comerciais.

7.1.4. Em nenhuma hipótese será admitida a identificação da Licitante, sob pena de desclassificação.

7.1.5. O valor inserido no sistema sempre será pelo **Valor Total Global**, conforme **ANEXO II (MODELO DE PROPOSTA COMERCIAL)** respectivamente, considerando todos os itens descritos.

7.1.6. Nos preços deverão estar inclusos, além das taxas, impostos e encargos, os valores pertinentes a todas as despesas e demais custos que possam influir direta ou indiretamente na prestação de serviços, objeto da presente licitação.

7.1.7. O valor proposto para o fornecimento será de exclusiva e total responsabilidade da Licitante, sendo considerado como justo e suficiente para a contratação oriunda da presente licitação.

7.1.8. No caso de empate entre 2 (dois) ou mais lances, o desempate se fará automaticamente pelo sistema, com base no horário do primeiro lance cadastrado.

7.1.9. **PROPOSTA AJUSTADA**: Proposta detalhada (**ANEXO II**) 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 da Licitante:

7.1.9.1. Deverá constar a especificação detalhada do objeto;

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

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

7.1.10. A validade da proposta não poderá ser inferior a **90 (noventa) dias corridos** a contar da data de estabelecimento do valor final negociado. Não sendo indicado o prazo de validade, fica subentendido como de 90 (noventa) dias corridos.

7.1.11. Caso haja o vencimento da validade da proposta sem que a licitação tenha sido homologada e adjudicada e o contrato ou instrumento equivalente assinado, esta ficará automaticamente prorrogada, exceto se houver manifestação contrária formal da Licitante, pelo e-mail licitacao.gms@sp.senac.br, na data de vencimento da proposta, dirigida à Comissão de Licitação, caracterizando seu declínio em continuar na licitação.

7.1.12. 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 de Licitação.

## 8. ESCLARECIMENTOS DE DÚVIDAS:

8.1. Os interessados poderão encaminhar solicitação de esclarecimentos, por escrito, até às **23h59 do dia 11 de dezembro de 2025**, por meio do Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, na aba "Mural", no campo "**ESCLARECIMENTOS**".

8.2. Os esclarecimentos de dúvidas registrados no Portal de Compras e Contratações do Senac São Paulo deverão ser exclusivamente para questões relativas à presente licitação.

8.2.1. Não serão reconhecidas dúvidas encaminhadas por outro meio que não seja o Portal de Compras e Contratações do Senac São Paulo.

8.3. As questões formuladas serão respondidas, por escrito, a todos os interessados, até o dia **12 de dezembro de 2025**, por meio do Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, na aba "Mural", no campo "**ESCLARECIMENTOS**". Não serão fornecidos esclarecimentos verbais por funcionários do Senac em quaisquer fases da presente licitação.

8.4. Os pedidos de esclarecimentos não suspendem os prazos previstos na licitação.

8.5. Caso a resposta ao esclarecimento resulte em modificação do presente Edital, será providenciada nova divulgação na mesma forma de sua divulgação inicial, além

do cumprimento dos mesmos prazos dos atos e procedimentos originais, exceto quando a alteração não comprometer a formulação das propostas.

8.6. Os esclarecimentos formulados, bem como suas respostas, passarão a integrar o presente Edital, independentemente de sua transcrição.

8.7. Não sendo formuladas solicitações de esclarecimentos e/ou informações até a data estabelecida, ocorrerá a preclusão do direito de apresentar quaisquer questionamentos ao presente Edital, suas cláusulas e anexos.

8.8. É de responsabilidade do interessado e de cada Licitante o acompanhamento de todas as informações no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, durante todo o processo licitatório, ficando desonerado o Senac da obrigação de prestar informação por qualquer outro meio de comunicação.

## 9. ABERTURA DAS PROPOSTAS ELETRÔNICAS

9.1. Às **10h00 do dia 15 de dezembro de 2025**, proceder-se-á à abertura das propostas de preços no sistema eletrônico.

9.2. 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.

9.2.1. Caso o Pregoeiro opte por realizar análise de propostas, da decisão de desclassificação somente caberá pedido de reconsideração ao Pregoeiro, a ser enviado exclusivamente por meio do Sistema Eletrônico, acompanhado da justificativa de suas razões, no **prazo de 3 (três) minutos** a contar do momento em que vier a ser disponibilizada no sistema eletrônico a decisão a ser impugnada.

9.2.2. O Pregoeiro analisará e decidirá, **no mesmo prazo**, salvo motivos que justifiquem a sua prorrogação, sendo-lhe facultado, para tanto, suspender a

sessão, registrar e disponibilizar a decisão no Sistema Eletrônico para acompanhamento em tempo real das Licitantes.

9.2.3. Havendo necessidade, o Pregoeiro poderá suspender a sessão, informando no "chat" a nova data e horário para continuidade.

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

9.2.5. 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.

9.3. **ABERTURA DA FASE DE LANCES E NEGOCIAÇÃO**

9.3.1. A disputa de lances ocorrerá em modo aberto, conjuntamente, com critério de julgamento **MENOR PREÇO GLOBAL** e terá início às **10h00 do dia 15 de dezembro de 2025**.

9.3.2. 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.

9.3.3. A formulação de lances será efetuada, exclusivamente, por meio do Sistema Eletrônico e em campo específico, sendo que os valores lançados via "chat" serão desconsiderados.

9.3.4. Todos os lances oferecidos serão registrados pelo Sistema Eletrônico, que indicará o lance de menor valor para acompanhamento em tempo real pelas Licitantes.

9.3.5. O Sistema Eletrônico não identificará os autores dos lances aos demais participantes durante o transcurso da sessão.

9.3.6. A Licitante poderá ofertar novo lance, desde que inferior ao último por ela ofertado e registrado no Sistema Eletrônico.

9.3.7. Na hipótese de haver lances iguais, prevalecerá como de menor valor o lance que tiver sido primeiramente registrado.

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

9.3.9. A etapa de lances terá duração de **10 (dez) minutos** e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos **últimos 2 (dois) minutos** do período de duração da sessão.

9.3.10. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de **2 (dois) minutos** e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

9.3.11. Não havendo novos lances na forma estabelecida nos subitens anteriores, a sessão de disputa encerrar-se-á automaticamente.

9.3.12. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá a Comissão Permanente de Licitação, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

9.3.13. Durante a sessão, as Licitantes serão informadas, em tempo real, sobre o valor do menor lance registrado, sem identificação da Licitante.

9.3.14. Encerrada a etapa de lances, o Sistema Eletrônico divulgará a nova grade ordenatória, contendo a classificação final, em ordem crescente de valores. Para essa classificação será considerado o último preço admitido de cada Licitante.

9.3.15. Após o encerramento da etapa de lances, o Pregoeiro poderá encaminhar, pelo Sistema Eletrônico, contraproposta à Licitante que tenha apresentado o lance mais vantajoso, para que seja obtida uma melhor proposta, observando o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no Edital.

9.3.16. A **negociação** será realizada por meio do Sistema Eletrônico, podendo ser acompanhada pelas demais licitantes.

9.3.17. O critério de **aceitabilidade** dos preços ofertados será o de compatibilidade com os preços dos insumos e salários praticados no mercado, coerentes com a execução do objeto ora licitado, acrescidos dos respectivos encargos sociais e benefícios e despesas indiretas (BDI).

9.3.18. O Pregoeiro poderá, a qualquer momento, solicitar às Licitantes a composição de preços unitários de serviços e/ou de materiais/equipamentos, bem como os demais esclarecimentos que julgar necessário para comprovação da exequibilidade dos preços apresentados, sob pena de desclassificação.

9.3.19. Encerrada a fase de lances e após a negociação, se houver, o Pregoeiro solicitará à empresa classificada em primeiro lugar o envio da **Proposta Comercial atualizada** pelo Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, que deverá ser encaminhada no prazo por ele estabelecido, contendo o carimbo do CNPJ, nome e CPF do representante e sua assinatura, para análise e aprovação.

9.3.20. Caso não seja apresentada a Proposta Comercial atualizada, a Comissão Permanente de Licitação poderá convocar o segundo menor lance e, se necessário, observada a ordem crescente de preço, as Licitantes dos demais lances, desde que atendam ao critério de aceitabilidade estabelecido no Edital.

9.4. **ENVIO DA PROPOSTA DE PREÇOS AJUSTADA E DOS DOCUMENTOS DE HABILITAÇÃO**

9.4.1. Ordenados os lances em forma crescente de preço, o Pregoeiro determinará a Licitante classificada em primeiro lugar para, **em até 2 (duas) horas ou em prazo acordado dentro da própria sessão** disponibilizar **a Proposta Ajustada** conforme previsto no **subitem 7.1.9** e os **Documentos de Habilitação** conforme previsto no **Item 6 seus subitens** deste Edital.

9.4.2. O prazo estabelecido poderá ser prorrogado por solicitação escrita e justificada da Licitante dentro do próprio sistema, formulada antes de findo o prazo, e formalmente aceita pelo pregoeiro.

9.4.3. Caso a Licitante possua o registro cadastral atualizado e as exigências atendidas, sua habilitação será reconhecida.

9.4.4. Será **inabilitada** a Licitante que deixar de apresentar ou apresentar em desacordo qualquer um dos documentos exigidos no **item 6** deste Edital, ou, quando for o caso, estar com seu respectivo **registro cadastral desatualizado e não o atualizar no prazo concedido pela Comissão Permanente de Licitação**.

9.4.4.1. Na hipótese de inabilitação, caberá à Comissão Permanente de Licitação autorizar o Pregoeiro a convocar a Licitante do segundo menor lance e, se necessário, observada a ordem crescente de preço, as Licitantes dos demais lances, desde que atendam ao critério de aceitabilidade estabelecido neste Edital.

9.4.4.2. O Pregoeiro poderá adotar os mesmos critérios de negociação descritos no **item 9**.

9.4.5. Na hipótese de inabilitação de todos as Licitantes ou de desclassificação de todas as propostas, a Comissão Permanente de Licitação poderá, a seu exclusivo critério, fixar prazo comum a todas as Licitantes para retificações, livres das causas que deram origem à inabilitação ou à desclassificação.

9.5. **DA HABILITAÇÃO COM REGISTRO CADASTRAL**

9.5.1. A Licitante que estiver com o registro cadastral **ATUALIZADO** no Cadastro de Fornecedores do Senac São Paulo poderá ser dispensada da apresentação dos **documentos de habilitação jurídica e regularidade fiscal**, ficando obrigatória a apresentação dos demais documentos exigidos no **item 6**.

9.5.2. A Licitante que estiver com o registro cadastral desatualizado poderá proceder à respectiva atualização acessando o Cadastro de Fornecedores no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, até a **data de abertura**.

9.5.3. Quaisquer informações ou dúvidas inerentes ao registro cadastral deverão ser encaminhadas nos termos do **subitem 8.1**.

9.5.4. Caso a Licitante não utilize as hipóteses do registro cadastral, deverá cumprir todas as exigências previstas no **item 6** (Documentos de Habilitação).

## 10. DECLARAÇÃO DA LICITANTE VENCEDORA

10.1. Realizada a análise nos documentos de habilitação, da proposta ajustada e das amostras (quando houver), o Pregoeiro indicará a Licitante vencedora e o processo será encaminhado à autoridade competente para homologação e adjudicação.

## 11. DOS RECURSOS

11.1. Divulgada a(s) vencedora(s) por decisão da Comissão Permanente de Licitação, a Licitante que dela discordar terá o prazo de **até 5 (cinco) minutos** para manifestar sua intenção de interpor recurso, em campo próprio do Sistema Eletrônico. A partir da aceitabilidade do recurso, a Licitante terá o prazo de **2 (dois) dias úteis** para apresentação das razões da interposição do recurso também no Sistema Eletrônico.

11.2. Interposto o recurso nos termos do **subitem 11.1**, dele se dará ciência às demais licitantes pelo Sistema Eletrônico, que poderão no mesmo prazo de até 2 (dois) dias úteis, para apresentar suas contrarrazões no Sistema Eletrônico. **O recurso terá efeito suspensivo**.

11.3. A falta de manifestação imediata e motivada da Licitante, bem como a não apresentação de documentos comprobatórios que instruam o recurso no prazo previsto no **subitem 11.1**, implicará a renúncia do direito de recorrer.

11.4. Na contagem dos prazos estabelecidos nos **subitens 11.1 e 11.2**, excluir-se-á o dia de início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos aqui referidos, em dia de funcionamento da Sede da Administração Regional do Senac São Paulo, localizada na Rua Dr. Vila Nova, 228, 7º andar, bairro Vila Buarque, São Paulo/SP.

11.5. O recurso interposto em desacordo com as condições estabelecidas neste Edital não será conhecido.
11.6. O acolhimento do recurso pela autoridade competente somente invalidará os atos insuscetíveis de aproveitamento.

## 12. SANÇÕES APLICÁVEIS NO PROCEDIMENTO LICITATÓRIO

12.1. A Licitante vencedora que, injustificadamente, recusar-se a assinar o contrato ou o instrumento equivalente, em prazo estipulado pela Comissão Permanente de Licitação, 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, pelo período de até **3 (três) anos.**

12.2. A Licitante perderá o direito de licitar com o Senac nas seguintes hipóteses:

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

b) Fraudar a licitação ou praticar ato fraudulento na execução do contrato ou instrumento equivalente.

c) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.
d) Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.
e) Praticar ato lesivo previsto no artigo 5° da Lei n 12.846, de 1.° de agosto de 2013.

12.3. 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.

12.4. O descumprimento total ou parcial das condições, prazos e obrigações contratuais, relacionadas à execução do objeto, poderá ensejar a aplicação das sanções previstas no contrato ou instrumento equivalente, sem prejuízo da responsabilização civil e penal, garantindo-se em qualquer hipótese o direito ao contraditório e à ampla defesa.

## 13. PROTEÇÃO DE DADOS PESSOAIS

13.1. O Senac tem compromisso com a privacidade e a proteção de dados pessoais de seus alunos, colaboradores, fornecedores, clientes e parceiros. E, nesse sentido, o Senac envida seus melhores esforços para, no tratamento de dados pessoais decorrente deste Edital, observar integralmente a legislação aplicável, em especial a

Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais ("LGPD"), comprometendo-se, na qualidade de controlador, a:

a) Cumprir as obrigações estabelecidas pela LGPD, tratando sempre o mínimo de dados pessoais necessários para atingir as finalidades deste Edital;

b) Adotar medidas razoáveis para informar empregados e terceiros sobre cuidados e responsabilidades resultantes de normas de proteção de dados pessoais;

c) Envidar esforços razoáveis para garantir que os dados pessoais tratados estejam atualizados e sejam relevantes em todas as circunstâncias, enquanto estiverem sob sua custódia ou sob seu controle, na medida em que tenha capacidade de fazê-lo;

d) Notificar o titular de dados pessoais e as autoridades acerca do tratamento não autorizado ou ilegal, perda, destruição, dano, alteração ou divulgação não autorizada, bem como qualquer violação de medidas de segurança em relação a dados pessoais cujo tratamento decorra deste Edital; e

e) Disponibilizar avisos de privacidade para ampliar a transparência e confiabilidade acerca do tratamento de dados pessoais realizado.

13.2. Ao participar do processo licitatório objeto deste Edital, a Licitante, por seus representantes legais e sob as penas da lei, declara como verdadeiros quaisquer dados pessoais informados na Documentação de Habilitação e/ou decorrentes do previsto neste Edital, responsabilizando-se por esta garantia e pela legalidade do compartilhamento dos dados pessoais com o Senac nos termos da legislação aplicável, em particular da LGPD. A Licitante, compromete-se, ainda, a não comunicar, revelar, disponibilizar ou utilizar dados pessoais aos quais tiver acesso em razão de sua participação no processo licitatório para finalidades distintas daquelas que motivaram o seu acesso, responsabilizando-se integral e exclusivamente pelo pleno atendimento desta obrigação.

13.3. A Licitante declara, por seus representantes legais e sob as penas da lei, que conhece e cumpre integralmente as disposições da LGPD no que toca o tratamento de dados pessoais necessário para a condução de seu negócio e execução do contrato objeto desta Licitação, particularmente que (i) observa as obrigações estabelecidas pela LGPD, garantindo, inclusive, a origem lícita e/ou necessidade dos dados pessoais tratados; (ii) adota medidas razoáveis para informar empregados e terceiros sobre

cuidados e responsabilidades resultantes de normas de proteção de dados pessoais; (iii) possui procedimento que permite notificar o Senac acerca do tratamento não autorizado ou ilegal, perda, destruição, dano, alteração ou divulgação não autorizada, bem como qualquer violação de medidas de segurança em relação a dados pessoais cujo tratamento decorra deste Edital e futuro contrato; e (iv) implementou mecanismos para cumprimento de solicitações envolvendo tratamento de dados pessoais pelos titulares e autoridades, e mitigação de riscos, podendo, inclusive, cooperar com o Senac nesse sentido.

13.4. A Licitante reconhece que, nos termos da legislação aplicável e políticas de privacidade e segurança da informação do Senac, bem como em decorrência deste Edital, dados pessoais serão tratados, de forma segura e em ambiente com acesso restrito, para fins especialmente de viabilizar (i) a participação na Licitação, (ii) a contratação, a condução e gestão das atividades relacionadas ao objeto da Licitação; e (iii) o contato do Senac por qualquer meio, inclusive para participação em processos licitatórios no futuro. Declara, ainda, ciência de que os dados pessoais podem ser, nos termos da lei, compartilhados pelo Senac com outras entidades como auditores, prestadores de serviços de controle de acesso às dependências do Senac, órgãos do governo, e/ou outros terceiros, inclusive para fins de transparência, evidência da lisura do processo licitatório e atendimento a dispositivos da Lei de Acesso à Informação, sobretudo para cumprimento de obrigações legais do Senac, execução do contrato, exercício regular de direitos e atingimento de interesses legítimos.

13.5. Em caso de dúvidas acerca do tratamento de dados pessoais e/ou para exercer os direitos previstos na LGPD, como de acesso, retificação e exclusão, o titular de dados pessoais e/ou seu representante poderão entrar em contato com o encarregado de proteção de dados do Senac São Paulo em https://www.sp.senac.br/fale-com-a-gente/privacidade-de-dados.

## 14. DA LEI ANTICORRUPÇÃO

14.1. A Licitante deverá atender às disposições contidas na Lei nº 12.846/2013 – Lei Anticorrupção, motivo pelo qual durante todo o período de vigência da contratação, conduzirá suas práticas comerciais de forma ética e em conformidade com os preceitos legais aplicáveis, não podendo dar, oferecer, pagar, prometer pagar ou autorizar o pagamento, direta e indiretamente, de qualquer valor, a quem quer que seja, com a finalidade de influenciar qualquer ato ou decisão, ou para assegurar qualquer vantagem indevida, ou direcionar negócios, e que violem o estabelecido na Lei Anticorrupção.

## 15. DISPOSIÇÕES GERAIS

15.1. Todas as informações da presente licitação, tais como esclarecimentos de dúvidas, erratas, julgamentos, recursos, resultados e homologação, dentre outras, serão comunicadas pelo site www.sp.senac.br/sites/licitacao. Sendo de responsabilidade de cada Licitante o devido acompanhamento e os atos praticados.

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

15.3. Caso as Licitantes declaradas vencedoras da licitação optem em fornecer os materiais/equipamentos ou prestar os serviços objeto da presente licitação por meio de estabelecimento filial, deverão realizar o cadastro ou atualização respectiva no Cadastro de Fornecedores no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, apresentando os documentos atualizados elencados no **subitem 6** em relação à filial eleita, bem como, documentos de qualificação técnica, quando houver, exceto aqueles que pela própria natureza ou por determinação legal, forem comprovadamente emitidos apenas em favor do estabelecimento matriz ou cuja validade abranja todos os estabelecimentos da empresa, no prazo de até 2 (dois) dias úteis a contar da data de solicitação do Senac.

15.4. Se as Licitantes vencedoras não apresentarem a documentação exigida no subitem anterior, o faturamento deverá ser realizado por meio de sua sede.

15.5. As Licitantes vencedoras deverão manter as condições que propiciaram a sua habilitação e qualificação, facultando-se ao Senac, a seu exclusivo critério, realizar diligência no endereço apresentado pelas vencedoras, para comprovação de todas as exigências descritas no Edital, bem como exigir a renovação cadastral, no ato da assinatura do contrato ou instrumento equivalente, no todo ou em parte, dos documentos de habilitação e qualificação.

15.6. O desatendimento de exigências formais não essenciais não importará no afastamento da Licitante, desde que seja possível a aferição da sua qualificação ou a exata compreensão da sua proposta.

15.7. O Senac poderá exigir a prestação de garantia contratual e, conforme o caso, de garantia adicional, nos termos que vierem a ser estabelecidos no contrato ou instrumento equivalente.

15.8. A Comissão 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.

15.9. A Comissão 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.

15.10. A Comissão de Licitação poderá, no interesse do Senac 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.

15.11. 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.

15.12. Admitir-se-á a continuidade do contrato ou instrumento equivalente 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 o **Regulamento de Licitações e Contratos do Senac São Paulo**, e ainda, que sejam mantidas as condições inicialmente estabelecidas.

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

15.14. A inobservância ao **Regulamento de Licitações e Contratos do Senac São Paulo** pode ensejar, em caso de comprovado prejuízo ao patrimônio do Senac, 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.

15.15. Os prepostos da Licitante vencedora não terão vínculos empregatícios e previdenciários de qualquer natureza com o Senac.

15.16. 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 e/ou terceiros, em decorrência da execução indevida do objeto desta licitação.

15.17. A Licitante declara ter ciência e se compromete a cumprir os princípios e regras contidos no Código de Ética do Senac São Paulo, disposto no site: http://sisnormas.sp.senac.br/sisnormas/downloads/codigo_de_etica_e_conduta_profissional_do_senac.

15.18. Considerando as medidas de segurança e boas práticas adotadas pelo Senac São Paulo, será de responsabilidade da Licitante a confirmação do recebimento dos e-mails enviados para o endereço eletrônico licitacao.gms@sp.senac.br. O Senac não se responsabilizará por e-mails não recebidos e não confirmados pela Licitante, independente do motivo que o ensejou.

15.19. Fica eleito o Foro da Comarca da Capital do Estado de São Paulo, para dirimir quaisquer dúvidas referentes ao presente Edital.

15.20. Fazem parte integrante deste Edital, os seguintes Anexos:
Anexo I – Termo de Referência
Anexo II – Proposta Comercial
Anexo III – TGC "Termo Geral de Contratação"

São Paulo, 05 de dezembro de 2025.

**Serviço Nacional de Aprendizagem Comercial – Senac**
Administração Regional no Estado de São Paulo
Gerência de Materiais e Serviços

**PREGÃO ELETRÔNIOCO - PEE 2025000116**

**TERMO DE REFERÊNCIA**

**ANEXO I**

## 1 - DESCRIÇÃO PROPOSTA DE PRODUTO (LICENCIAMENTO)

1.1. Aquisição de Software de Segurança para Estações de Trabalho, com proteção avançada e gestão centralizada, incluindo funcionalidades de Detecção e Resposta Estendida.

1.2. Aquisição de Solução de Segurança para Cargas de Trabalho Híbridas, Servidores e Estações de Trabalho, com Detecção e Resposta Estendida.

1.3. Aquisição de Solução de Gerenciamento de Risco Cibernético e Identificação de Exposição Externa com Detecção e Resposta Estendida.

1.4. Aquisição de Solução de Proteção Avançada para Dispositivos Móveis (Mobile Security).

1.5. Aquisição de Solução de Proteção para E-Mail e Colaboração (Email and Collaboration Security).

1.6. Aquisição de Solução de Proteção Avançada para Áreas de Armazenamento em Nuvem (File Security).

Conforme informações descritas na tabela abaixo:

| Item | Descrição | Qtd |
|---|---|---|
| 1 | TrendMicro VisionOne - Endpoint Security (Essentials) | 30507 |
| 2 | TrendMicro Workload Security - PRO | 1840 |
| 3 | TrendMicro Cyber Risk Exposure Management Core | 3027 |
| 4 | TrendMicro Mobile Security | 100 |
| 5 | TrendMicro VisionOne Email and Collaboration Security | 1241 |
| 6 | TrendMicro VisionOne File Security per 500K | 2 |

**Gerência de Materiais e Serviços**
**Senac São Paulo**

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
E-mail: licitacao.gms@sp.senac.br
www.sp.senac.br

## 2. DISPOSIÇÕES GERAIS SOFTWARES

### 2.1. DISTRIBUIÇÃO E CONFIGURAÇÃO DE TENANTS

2.1.1. Será necessária a configuração e distribuição de até 30 tenants na solução, com divisão e alocação específica para cada estado, de forma a garantir o controle e o gerenciamento descentralizado de cada unidade.

### 2.2. REQUISITOS TÉCNICOS PARA AQUISIÇÃO DE SOFTWARE DE SEGURANÇA PARA ESTAÇÕES DE TRABALHO (ENDPOINT ESSENCIAL)

2.2.1. A solução deverá ser entregue na modalidade SaaS;

2.2.2. Possuir console Web para gerenciamento e administração da ferramenta;

2.2.3. A solução deverá ser toda de um único fabricante, não sendo aceitos agentes ou plug-ins adicionais;

2.2.4. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall de Host, Host IPS, Controle de Aplicações, Controle de dispositivos e XDR (Extended Detection and Response) em um único agente.

2.2.5. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows 7 SP1 32/64-bit
- Windows 8.1 32/64-bit
- Windows 10 Enterprise Version;
- Windows Embedded Standard 7 sp1
- Windows 10 Iot Version
- Windows Server 2008 R2 SP1 64-bit
- Windows StorageServer 2008 R2 64-bit
- Windows HPC Server 2011 64-bit
- Windows server 2012 64-bit
- Windows 11 Home and Pro.
- Windows 11 Enterprise
- MacOS Sequoia
- MacOS Sonoma
- MacOS Ventura
- MacOs Monterey
- MacOs Big sur
- MacOs Catalina

- MacOS Mojave
- MacOS High
- MacOs Sierra
- OS X El Capitan

2.2.6. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso.

2.2.7. Deve prover visibilidade de casos de insucesso de varredura, para tomada de ações pontuais;

2.2.8. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, Ransomware entre outros;

2.2.9. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

- Processos em execução em memória principal (RAM);
- Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando, tais como DOS ou Shell;
- Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;
- Arquivos recebidos por meio de programas de comunicação instantânea, como: MSN messenger, yahoo messenger, google talk, icq, entre outros.

2.2.10. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript e VBScript/Activex;

2.2.11. Deve possuir detecção heurística de vírus desconhecidos;

2.2.12. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual e agendada;

2.2.13. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

- Em tempo real de arquivos acessados pelo usuário;
- Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a

necessidade de escrita de arquivo;
- Manual, imediato ou programável, com interface gráfica personalizável, com opção de limpeza;

2.2.14. Automáticos do sistema com as seguintes opções:

- Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
- Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- Frequência: horária, diária, semanal e mensal;
- Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

2.2.15. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

2.2.16. Em caso de arquivos suspeitos, a solução deve ter a capacidade de enviar o artefato para um ambiente de sandbox na plataforma de XDR do próprio fabricante para identificar ameaças desconhecidas;

2.2.17. O módulo de análise de artefatos desconhecidos (sandbox) deve estar integrada à solução de XDR, sem necessidade de plugins adicionais;

2.2.18. O módulo de sandbox deve permitir a análise de arquivos submetidos diretamente dos agentes;

2.2.19. Em caso de ameaças desconhecidas detectadas pela sandbox, a solução deve ter a capacidade de adicionar os objetos suspeitos (hash de arquivo, IP, domínio e URL) numa lista de bloqueio automaticamente;

2.2.20. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

2.2.21. Deve permitir a utilização de repositórios locais de reputação e inteligência, para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

2.2.22. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web,

de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

2.2.23. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória das estações de trabalho, mitigando tais ações;

2.2.24. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos;

2.2.25. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

2.2.26. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

2.2.27. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

2.2.28. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

2.2.29. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de ofuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

2.2.30. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

2.2.31. Deve bloquear processos comuns associados a ransomware;

2.2.32. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios;

2.2.33. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

2.2.34. Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante;

2.2.35. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

2.2.36. Deve permitir atualização incremental da lista de definições de vírus;

2.2.37. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

2.2.38. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

2.2.39. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

2.2.40. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

2.2.41. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

2.2.42. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

2.2.43. Deve possibilitar instalação "silenciosa";

2.2.44. Deve permitir o bloqueio por nome de arquivo;

2.2.45. Deve permitir o travamento de pastas e diretórios;

2.2.46. Deve permitir o travamento de compartilhamentos;

2.2.47. Deve permitir o rastreamento e bloqueio de infecções;

2.2.48. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

2.2.49. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

2.2.50. Deve permitir a desinstalação através da console de gerenciamento da solução;

2.2.51. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

2.2.52. Deve permitir a deleção dos arquivos quarentenados;

2.2.53. Deve permitir remoção automática de clientes inativos por determinado período;

2.2.54. Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;

2.2.55. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

2.2.56. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

2.2.57. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

2.2.58. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory, tipo ou IP;

2.2.59. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

2.2.60. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

2.2.61. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

2.2.62. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

2.2.63. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;

2.2.64. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

2.2.65. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

2.2.66. Deve permitir a criação de usuários locais de administração da console de anti-malware;

2.2.67. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

2.2.68. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

2.2.69. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

2.2.70. Deve permitir a gerência de domínios separados para usuários

previamente definidos;

2.2.71. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido no console de administração;

2.2.72. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

2.2.73. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

2.2.74. Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

2.2.75. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

2.2.76. Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

2.2.77. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

2.2.78. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

2.2.79. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;

2.2.80. Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

2.2.81. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

2.2.82. Deve permitir controle de permissão ou bloqueio para dispositivos

que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

2.2.83. Deve ser capaz de realizar a detecção e proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

- Windows 7 SP1 32/64-bit
- Windows 8.1 32/64-bit
- Windows 10 Enterprise Version;
- Windows 10 Iot Version
- Windows Server 2008 R2 SP1 64-bit
- Windows StorageServer 2008 R2 64-bit
- Windows HPC Server 2011 64-bit
- Windows server 2012 64-bit
- Windows 11 Home and Pro.
- Windows 11 Enterprise
- MacOS Sequoia
- MacOS Sonoma
- MacOS Ventura
- MacOs Monterey
- MacOs Big sur
- MacOs Catalina
- MacOS Mojave
- MacOS High

2.2.84. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

2.2.85. Deve possuir módulo Firewall de host, não sendo permitidas soluções que não possuam módulo próprio;

2.2.86. Não serão aceitas soluções que apenas gerenciam o Firewall do Windows;

2.2.87. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

2.2.88. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

2.2.89. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

2.2.90. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

2.2.91. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

2.2.92. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

2.2.93. O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

2.2.94. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;

2.2.95. O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

2.2.96. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

2.2.97. Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

2.2.98. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

2.2.99. As regras de controle de aplicação devem permitir as seguintes ações:
- Permissão de execução;
- Bloqueio de execução;
- Bloqueio de novas instalações.

2.2.100. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos;

2.2.101. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

2.2.102. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações;

2.2.103. Assinatura SHA-1 e SHA-256 do executável;

2.2.104. Atributos do certificado utilizado para assinatura digital do executável;

2.2.105. Caminho lógico do executável;

2.2.106. Base de assinaturas de cerificados digitais válidos e seguros.

2.2.107. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

2.2.108. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

2.2.109. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;

2.2.110. Deve permitir a busca por aplicações ou fabricante destas;

2.2.111. Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV;

2.2.112. A solução deverá por meio de agente único possibilitar a conexão com a plataforma de XDR do próprio fabricante de maneira nativa sem a necessidade de plug-ins ou agentes adicionais;

2.2.113. Esta conexão deverá garantir, sem qualquer configuração local, que o XDR esteja ativo e envie telemetria a plataforma;

2.2.114. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;

2.2.115. A solução deve possuir módulo de investigação, detecção e resposta integrados;

2.2.116. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades das máquinas do ambiente;

2.2.117. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

2.2.118. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

2.2.119. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

2.2.120. Ser capaz de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

2.2.121. Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

2.2.122. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;

2.2.123. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;

2.2.124. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

2.2.125. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

2.2.126. Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

2.2.127. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

2.2.128. O módulo de XDR deve atuar baseado em modelos de detecção de

ataques avançados e furtivos;

2.2.129. Os logs de detecções devem estar disponíveis no console por, pelo menos, 30 dias;

2.2.130. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações.

## 2.3. REQUISITOS TÉCNICOS PARA AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS, SERVIDORES E ESTAÇÕES DE TRABALHO COM DETECÇÃO E RESPOSTA ESTENDIDA.

2.3.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

- Windows Server 2003 SP1 e 2003 R2 SP2;
- Windows Server 2008 e 2008 R2;
- Windows Server 2012 e 2012 R2;
- Windows Server 2016;
- Windows Server 2019;
- Windows Server 2022;
- Windows 7 SP1;
- MacOs BIGsur ou superior;
- Red Hat Enterprise 5, 6, 7 e 8;
- CentOS 5, 6, 7 e 8;
- AIX 6.1, 7.1 e 7.2;
- Oracle Linux 5, 6, 7 e 8;
- SUSE Linux Enterprise Server 10, 11, 12 e 15;
- Ubuntu 10, 12, 14, 16, 18 e 20;
- Debian 6, 7, 8, 9 e 10;
- Rocky Linux 8;
- AlmaLinux 8;
- Cloud Linux 5, 6, 7 e 8;
- Solaris 10 1/13 Sparc;
- Solaris 10 1/13 (x86/x64);
- Solaris 11.2/ 11.3 Sparc;
- Solaris 11.2/ 11.3 (x86/x64);
- Solaris 11.4 (x86, x64 ou SPARC)
- Amazon Linux e Amazon Linux 2 (x64)

2.3.2. A console de gerenciamento deverá ser em nuvem, permitindo o gerenciamento das políticas de segurança através do acesso via Internet;

2.3.3. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Google Chrome, Internet Explorer e Firefox. Deve ainda suportar certificado digital para gerenciamento;

2.3.4. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, Microsoft Azure, Amazon Web Services e Google Cloud Platform;

2.3.5. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

2.3.6. A solução deverá permitir a entrega de agentes por regras de GPO e Script;

2.3.7. A console de administração deverá permitir o envio de notificações via SMTP;

2.3.8. Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria;

2.3.9. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

2.3.10. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

2.3.11. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

2.3.12. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;

2.3.13. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

2.3.14. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

2.3.15. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;

2.3.16. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

2.3.17. A solução de segurança ter a capacidade de identificar ataques em estruturas de container.

2.3.18. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

2.3.19. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar políticas de segurança;

2.3.20. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

2.3.21. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

2.3.22. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

2.3.23. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

2.3.24. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

2.3.25. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

2.3.26. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

2.3.27. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

2.3.28. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

2.3.29. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

2.3.30. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

2.3.31. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

2.3.32. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

2.3.33. A solução deverá mostrar quais máquinas estão usando determinada política;

2.3.34. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

2.3.35. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

2.3.36. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

2.3.37. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

2.3.38. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades

escolhendo o perfil ou o host;

2.3.39. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

2.3.40. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

2.3.41. A solução deverá ser capaz de executar by-pass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

2.3.42. A solução deverá ter a capacidade de se integrar com softwares de SIEMs, de modo a permitir enviar os seus logs para essas soluções;

2.3.43. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

2.3.44. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

2.3.45. Deve permitir enviar os relatórios para uma lista de contatos independente de login no console de administração;

2.3.46. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

2.3.47. Após a atualização deve ser informado o que foi modificado ou adicionado;

2.3.48. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

2.3.49. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

2.3.50. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

2.3.51. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

2.3.52. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

2.3.53. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

2.3.54. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

2.3.55. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

2.3.56. O fabricante deverá participar do programa "Microsoft Application Protection Program" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

2.3.57. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

2.3.58. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

2.3.59. A solução deve possuir API documentada para integração na esteira de automação;

2.3.60. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

2.3.61. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

2.3.62. A solução deve permitir desabilitar os módulos individualmente;

2.3.63. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de host IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

2.3.64. A console deverá possibilitar a integração com o Microsoft Active Directory, listando as máquinas e grupos existentes na estrutura;

2.3.65. Em caso de a solução ser ofertada em nuvem, deve ser compliance com ISO 27001, ISO 27014, ISO 27017 e SOC 2 Type II;

2.3.66. Os ambientes em nuvem providos pelo fabricante devem passar por testes de penetração de forma recorrente como para garantir a segurança da solução provida.

2.3.67. Deve possuir módulo avançado de antimalware contra ameaças;

2.3.68. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

2.3.69. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

2.3.70. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

2.3.71. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

2.3.72. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

2.3.73. Deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

2.3.74. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

2.3.75. A solução deverá oferecer escanear processos em memória em busca

de Malware;

2.3.76. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

2.3.77. O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;

2.3.78. A solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

2.3.79. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

2.3.80. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

2.3.81. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

2.3.82. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

2.3.83. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

2.3.84. Deve possibilitar o controle do consumo de CPU durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

2.3.85. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

2.3.86. Deve possuir capacidade de detectar ameaças por comportamento;

2.3.87. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

2.3.88. Deve possuir módulo de proteção contra URLs maliciosas;

2.3.89. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

2.3.90. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

2.3.91. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;

2.3.92. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

2.3.93. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

2.3.94. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

2.3.95. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

2.3.96. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

2.3.97. Deve possuir módulo Firewall de Host, não sendo permitidas soluções que não possuam módulo próprio;

2.3.98. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

2.3.99. Não serão aceitas soluções que apenas gerenciam o firewall Windows da máquina;

2.3.100. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

2.3.101. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

2.3.102. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

2.3.103. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;

2.3.104. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

2.3.105. Precisa ter a capacidade de definição de regras para contextos específicos;

2.3.106. Facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;

2.3.107. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

2.3.108. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

2.3.109. O firewall deverá ser stateful bidirecional;

2.3.110. O firewall deverá permitir liberar ou apenas logar eventos;

2.3.111. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

2.3.112. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

2.3.113. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

2.3.114. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

2.3.115. Deverá realizar pseudo stateful em tráfego UDP;

2.3.116. Deverá logar a atividade stateful;

2.3.117. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

2.3.118. Deverá permitir limitar o número de meias conexões vindas de um computador;

2.3.119. Deverá prevenir ack storm;

2.3.120. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

2.3.121. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período configurado pelo administrador;

2.3.122. Deverá permitir criar lista de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede;

2.3.123. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

2.3.124. Deve prover proteção contra vulnerabilidades de Sistemas Operacionais e Aplicações;

2.3.125. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

2.3.126. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do Sistema Operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

2.3.127. A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;

2.3.128. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

2.3.129. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

2.3.130. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

2.3.131. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

2.3.132. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

2.3.133. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

2.3.134. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

2.3.135. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

2.3.136. Regras de IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

2.3.137. Regras de IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

2.3.138. Deverá ser capaz de inspecionar tráfego criptografado de entrada;

2.3.139. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI

fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

2.3.140. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

2.3.141. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

2.3.142. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

2.3.143. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

2.3.144. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

2.3.145. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

2.3.146. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

2.3.147. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;

2.3.148. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

2.3.149. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

2.3.150. As regras devem ser atualizadas automaticamente pelo fabricante;

2.3.151. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

2.3.152. Deve ser capaz de realizar monitoramento da integridade dos Servidores;

2.3.153. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

2.3.154. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

2.3.155. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

2.3.156. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

2.3.157. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

2.3.158. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

2.3.159. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

2.3.160. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

2.3.161. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real- time para ambiente Linux;

2.3.162. Deverá logar e colocar em relatório todas as modificações que ocorram;

2.3.163. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

2.3.164. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

2.3.165. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

2.3.166. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

2.3.167. Deve possuir módulo de inspeção de logs para Servidores;

2.3.168. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

2.3.169. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

2.3.170. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

2.3.171. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

2.3.172. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

2.3.173. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

2.3.174. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

2.3.175. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

2.3.176. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

2.3.177. Deverá logar cada violação e colocar em relatório todas as violações

relevantes que ocorram;

2.3.178. As regras poderão ser modificadas por severidade de ocorrência de eventos;

2.3.179. As regras devem se atualizar automaticamente pelo fabricante;

2.3.180. Permitir modificação pelo administrador em regras para adequação ao ambiente.

2.3.181. Deve possuir módulo de controle de aplicações;

2.3.182. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

2.3.183. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;

2.3.184. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

2.3.185. A console deverá exibir eventos de no mínimo 30 dias;

2.3.186. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;

2.3.187. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

2.3.188. Deve prover módulo de detecção e resposta estendida – XDR em um único agente;

2.3.189. A solução deve possuir módulo de investigação, detecção integrados;

2.3.190. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

2.3.191. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções,

atualizações e disponibilidade;

2.3.192. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

2.3.193. O módulo de XDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

2.3.194. Os logs de detecções devem estar disponíveis no console por, pelo menos, 30 dias;

2.3.195. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

2.3.196. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados no console, ainda que estas não sejam detectadas como maliciosas;

2.3.197. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

2.3.198. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

2.3.199. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

2.3.200. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

2.3.201. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

2.3.202. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

2.3.203. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto

para o site da organização;

2.3.204. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

2.3.205. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

## 2.4. REQUISITOS TÉCNICOS PARA AQUISIÇÃO DE SOLUÇÃO DE PROTEÇÃO AVANÇADA PARA DISPOSITIVOS MÓVEIS (MOBILE SECURITY)

2.4.1. A solução deverá ser fornecida na modalidade SaaS (Software as a Service);

2.4.2. A solução deverá prover proteção e gerenciamento proativo de dispositivos móveis, incluindo smartphones, tablets e Chromebooks;

2.4.3. A solução deverá integrar tecnologias avançadas de detecção de ameaças móveis para auxiliar na mitigação de riscos de segurança;

2.4.4. A solução deverá realizar análise contínua do comportamento dos aplicativos instalados nos dispositivos, detectando atividades suspeitas ou maliciosas;

2.4.5. A solução deverá detectar proativamente aplicativos maliciosos, aplicativos que realizem vazamento de dados e aplicativos vulneráveis;

2.4.6. A solução deverá detectar conexões Wi-Fi maliciosas, incluindo ataques man-in-the-middle, HTTPS stripping e uso de criptografia fraca;

2.4.7. A solução deverá emitir alertas em tempo real no console administrativo e no próprio dispositivo protegido;

2.4.8. A solução deverá realizar verificação das configurações de segurança do dispositivo, identificando violações e não conformidades;

2.4.9. A solução deverá prover proteção baseada em reputação web (Web Reputation), bloqueando acesso a sites maliciosos e prevenindo exploração de vulnerabilidades;

2.4.10. A solução deverá incluir módulo de Mobile Device Director (MDD) integrado para gerenciamento nativo de dispositivos móveis, sem

necessidade de MDM de terceiros;

2.4.11. A solução deverá, opcionalmente, suportar integração com plataformas de MDM (Mobile Device Management) de terceiros, permitindo gerenciamento centralizado;

2.4.12. A solução deverá possuir compatibilidade com Microsoft Entra ID (antigo Azure AD) para autenticação e controle de acesso centralizado;

2.4.13. A solução deverá disponibilizar console web centralizada para gerenciamento, monitoramento e geração de relatórios;

2.4.14. A console administrativa deverá ser acessível via navegador web (Google Chrome ou equivalente), com criptografia de comunicação TLS 1.2 ou superior;

2.4.15. A solução deverá possuir autenticação multifator (MFA) para acesso ao console de administração;

2.4.16. A solução deverá incluir aplicativo Mobile Security for Business, com agente nativo residente no dispositivo móvel para proteção em tempo real;

2.4.17. O agente deverá ser compatível com sistemas operacionais Android, iOS e ChromeOS;

2.4.18. O agente deverá permitir bloqueio remoto do dispositivo, limpeza segura (wipe) e localização via console administrativa;

2.4.19. A solução deverá gerar relatórios automáticos de status de segurança dos dispositivos gerenciados, enviando informações ao servidor Mobile Security;

2.4.20. A solução deverá apresentar painel de visibilidade contendo indicadores de conformidade, status de proteção, incidentes recentes e tendências de ameaças móveis;

2.4.21. A solução deverá permitir configuração de políticas de segurança por grupo, unidade organizacional, sistema operacional e tipo de dispositivo;

2.4.22. A solução deverá permitir o isolamento automático de dispositivos

comprometidos ou não conformes com as políticas de segurança;

2.4.23. A solução deverá gerar alertas automáticos via e-mail, console e API em caso de detecção de malware ou risco de segurança;

2.4.24. A solução deverá suportar APIs RESTful para integração com plataformas de orquestração e resposta (SOAR) e ferramentas de SIEM;

2.4.25. A solução deverá ser compatível com o modelo de créditos Trend Vision One™, com consumo flexível de recursos de acordo com o uso;

2.4.26. A solução deverá manter histórico de eventos, logs e registros de auditoria por, no mínimo, 90 (noventa) dias;

2.4.27. A solução deverá suportar exportação de logs e relatórios nos formatos CSV, JSON e PDF;

2.4.28. A solução deverá permitir definição de perfis de acesso distintos para administradores, analistas e operadores;

2.4.29. A solução deverá permitir configuração de alertas baseados em políticas de risco e comportamento anômalo;

2.4.30. A solução deverá possuir integração nativa com o console Trend Vision One™, permitindo correlação de eventos de segurança entre dispositivos móveis e demais camadas de proteção;

2.4.31. A solução deverá identificar comunicações suspeitas de aplicativos com servidores maliciosos ou de comando e controle (C&C);

2.4.32. A solução deverá identificar vulnerabilidades conhecidas no sistema operacional e aplicações, com recomendações de correção;

2.4.33. A solução deverá permitir geração de relatórios de conformidade para auditorias de segurança e privacidade;

2.4.34. A solução deverá suportar integração com plataformas corporativas de gerenciamento de identidades e acessos (IAM);

2.4.35. A solução deverá possuir mecanismos de atualização automática e contínua dos módulos de detecção;

2.4.36. A solução deverá utilizar inteligência de ameaças global do fabricante, com atualização constante de reputação e assinaturas;

2.4.37. A solução deverá permitir análise de comportamento de aplicativos para detecção de ameaças de dia zero e variantes desconhecidas;

2.4.38. A solução deverá disponibilizar modo de operação online e offline, garantindo proteção mesmo sem conexão contínua à internet;

2.4.39. A solução deverá garantir que todos os dados trafegados entre dispositivos, console e servidor sejam criptografados de ponta a ponta;

2.4.40. A solução deverá possuir suporte técnico e documentação completa em língua portuguesa, com portal de suporte e base de conhecimento disponíveis 24x7.

## 2.5. REQUISITOS TÉCNICOS PARA AQUISIÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE RISCO CIBERNÉTICO E IDENTIFICAÇÃO DE EXPOSIÇÃO EXTERNA COM DETECÇÃO E RESPOSTA ESTENDIDA

2.5.1. A solução deverá ser entregue na modalidade SaaS;

2.5.2. Deve coletar a telemetria das soluções descritas nos itens 2.1, 2.2, 2.3 e 2.4, a fim de aferir o nível de risco do ambiente do Senac;

2.5.3. A solução deverá ser toda de um único fabricante;

2.5.4. Deve ser capaz de escanear ao menos 10 diferentes domínios públicos do Senac, de forma a:

- Identificar e mapear as vulnerabilidades presentes nos domínios públicos;
- Identificar as portas que estão abertas a internet;
- Mapear a localização e hospedagem dos domínios;
- Identificar e listar os protocolos e serviços presentes em cada domínio;

2.5.5. Deve ser capaz de identificar comportamentos anômalos a nível de usuário, por meio de integração com os serviços de diretórios:

- Active Directory;
- Azure AD;

- OKTA;
- OpenLDAP;

2.5.6. Através desta integração deve mapear os usuários que representem risco ao ambiente do Senac;

2.5.7. A solução deve identificar possíveis comprometimentos de contas, apresentando os espectros de riscos atrelados a tais alertas;

2.5.8. A solução deve, com base na integração com os serviços de diretórios, identificar possíveis tentativas de comprometimento de contas, por meio de ataques de força bruta;

2.5.9. Deve alertar se a conta do usuário está inativa, ao menos, por mais de 100 dias;

2.5.10. Deve apresentar as máquinas em que uma conta de usuário foi utilizada para login;

2.5.11. Deve apresentar o perfil informativo de cada conta de usuário, sendo possível detalhar:
- Tipo de conta;
- Privilégio;
- Grupo pertencente;
- Nota de Risco cibernético;
- Status da conta;

2.5.12. Ao acessar o perfil da conta do usuário, deve ser possível disparar ação automatizada de forçar o reset de senha do usuário;

2.5.13. Por meio da integração com o Azure AD, deve ser capaz de mapear as requisições e tentativas de login, de acordo com a geolocalização do usuário;

2.5.14. Por meio da integração com o Azure AD, deve ser capaz de forçar o logout do usuário;

2.5.15. Deve identificar tentativas de login geograficamente impossíveis, por exemplo, um usuário realiza login a partir de São Paulo - Brasil e no mesmo dia tenta realizar login de outro País;

2.5.16. Deve listar as contas que apresentem autenticação vulnerável;

2.5.17. Deve possibilitar a criação de playbooks de ações automatizadas, a fim de:

- Resetar a senha do usuário;
- Desabilitar a conta do usuário;
- Reabilitar a conta do usuário;

2.5.18. Deve listar os aplicativos web acessados pelos usuários, apresentando-os de acordo com o nível de risco mapeado e ainda, quando aplicável, apontar a data do primeiro de vazamento de dados de cada empresa desenvolvedora da aplicação;

2.5.19. Deve listar as normas de conformidade a qual os aplicativos acessados estão de acordo;

2.5.20. Deve listar os usuários que acessaram cada aplicativo e elencar o número de visitas;

2.5.21. Deve ser possível que o Senac elenque os aplicativos que são sancionados e não sancionados para uso dos usuários;

2.5.22. Deve apontar a geolocalização dos acessos a aplicativos web realizados pelos usuários;

2.5.23. Deve apontar a categoria dos aplicativos web acessados pelos usuários;

2.5.24. Deve listar os aplicativos instalados nas máquinas do Senac, com base no agente instalado;

2.5.25. Deve listar as vulnerabilidades presentes nas máquinas do Senac, elencando cada uma de acordo com o nível de exploração identificado no ambiente;

2.5.26. Deve apresentar o nível de severidade de cada vulnerabilidade de acordo com a seguinte classificação:
- Nível Alto de potencial de exploração;
- Nível Médio de potencial de exploração;
- Nível Baixo de potencial de exploração;

2.5.27. Deve apresentar o CVSS score de cada vulnerabilidade com base no NIST - National Institute of Standards and Technology, e apontar as recomendações de remediação;

2.5.28. Deve suportar integração com soluções de escaneamento de vulnerabilidades, tais como:
- Tenable IO;

- Nessus PRO;
- Qualys;
- Rapid7 Nexpose;
- Tanium Comply;

2.5.29. A partir destas integrações, deve coletar as informações de mapeamentos de vulnerabilidades e gerar correlações com a solução;

2.5.30. Deve apresentar o nível de risco do ambiente, apontando quais ações devem ser mitigadas a fim de diminuir tal valor de risco;

2.5.31. Deve possuir os seguintes gráficos:
- Top 10 usuários com Risco;
- Top 10 vulnerabilidades mais críticas;
- Top 10 máquinas com maior nível de risco;
- Top 10 aplicativos mais acessados;

2.5.32. Ameaças existentes no ambiente com base na matriz do MITRE ATT&CK;

2.5.33. Deve mapear os dispositivos existentes na rede do Senac e apontar aqueles que são gerenciados pela solução;

2.5.34. Deve listar as contas de usuários que foram comprometidas e estão expostas na dark web.

2.5.35. Deve apresentar o nível de risco de cada máquina mapeada na rede do Senac, sendo possível:

- Apontar as vulnerabilidades existentes.
- Alertas de anomalias de acesso baseados comportamentos;
- Alertas de configuração de sistema;

2.5.36. Listar os aplicativos instalados, com respectivas versões, fabricantes e data de instalação;

2.5.37. Deve ser capaz de iniciar uma sessão de shell remota na máquina;

2.5.38. Deve ser capaz de tomar ação de isolamento da máquina, na qual restrinja a comunicação da máquina apenas com o endereço da plataforma de gerenciamento de risco;

2.5.39. Deve ser possível que scripts baseados em powershell e bash, sejam enviados as máquinas que possuam o agente instalado;

2.5.40. De acordo com o mapeamento de fases de um ataque baseado no MITRE ATT&CK, deverá apontar se existentes máquinas que estão sob alguma fase de ataque;

2.5.41. Deve apresentar panorama de risco do ambiente do Senac, sendo possível comparar tal valor de risco com base:
- Empresas do mesmo segmento;
- Empresas do mesmo tamanho, quanto a número de funcionários;

2.5.42. Deve possuir modelo de parametrização de risco associado aos padrões conhecidos de mercado, como o NIST. Não sendo aceitas soluções que utilizam métrica própria.

2.5.43. A análise de risco deve ser contínua e automatizada.

2.5.44. A plataforma deve monitorar atributos de ativos e padrões de comportamento para avaliar o valor empresarial com base na triade CIA conforme descrito no NIST SP 800-60.

2.5.45. A plataforma deve fornecer um índice global de risco;

2.5.46. Deve indicar os principais eventos que devem ser mitigados para diminuir a pontuação de risco do Senac;

2.5.47. A visibilidade de riscos deve detalhar quais são os principais alertas de segurança e associá-los às táticas do MITRE;

2.5.48. Deve ser possível identificar pontos de melhorias associados às camadas de proteção do ambiente do Senac;

## 2.6. REQUISITOS TÉCNICOS PARA AQUISIÇÃO DE SOLUÇÃO DE PROTEÇÃO PARA E-MAIL E COLABORAÇÃO (EMAIL AND COLLABORATION SECURITY)

2.6.1. A solução deverá possuir mecanismos de proteção multicamadas contra ameaças em serviços de e-mail, incluindo phishing, spoofing, BEC (Business Email Compromise), Account Takeover, spam, mail bomb, anexos e links maliciosos, e ameaças avançadas (APT ou zero-day);

2.6.2. Deverá possuir funcionalidades de sandbox, antimalware, reputação de URL, antispam e antiphishing;

2.6.3. Deverá realizar análise estática e dinâmica de mensagens e anexos;

2.6.4. O licenciamento deverá contemplar todas as funcionalidades, com direito a atualizações e correções durante a vigência do contrato;

2.6.5. A solução deverá integrar-se nativamente com Google Workspace e Microsoft 365, preferencialmente via API, sem necessidade de agentes locais;

2.6.6. Deverá suportar autenticação SAML;

2.6.7. Toda a solução deverá ser de um único fabricante e gerenciada por console única;

2.6.8. Deverá permitir o gerenciamento de múltiplos domínios de e-mail na mesma console;

2.6.9. A solução deverá ser 100% em nuvem do fabricante, em modelo multi-tenant, garantindo a segregação e confidencialidade dos dados do contratante;

2.6.10. Deverá operar em regime 24x7 com disponibilidade mínima de 99% ao mês;

2.6.11. Toda comunicação deverá utilizar algoritmos criptográficos seguros;

2.6.12. Deverá prover proteção inbound de e-mails sem necessidade de appliance adicional;

2.6.13. Deverá permitir verificação e quarentena de mensagens suspeitas;

2.6.14. Deverá operar nos modos observação (somente análise) e proteção (bloqueio e quarentena);

2.6.15. A solução deverá empregar tecnologias de inteligência artificial e aprendizado de máquina para análise de comportamento e mitigação automática de incidentes;

2.6.16. Deverá analisar o comportamento de usuários e histórico de comunicação para aprimorar a detecção de ameaças;

2.6.17. Deverá possibilitar a utilização de feeds de reputação de domínios e

IPs;

2.6.18. Deverá permitir customização de mensagens de bloqueio e banners de alerta em e-mails suspeitos;

2.6.19. Deverá permitir que usuários reportem mensagens suspeitas, com posterior análise automatizada ou manual;

2.6.20. Deverá possuir quarentena de mensagens maliciosas, com retenção mínima de 30 dias;

2.6.21. Deverá manter logs e eventos sincronizados com o horário oficial de Brasília (GMT-3);

2.6.22. Deverá possibilitar o rastreamento e auditoria de acessos e ações sobre mensagens quarentenadas;

2.6.23. Deverá suportar integração com ferramentas de SIEM via Syslog ou protocolo equivalente;

2.6.24. Deverá ser capaz de identificar e bloquear anexos maliciosos, incluindo ransomware e ameaças de dia zero;

2.6.25. Deverá permitir bloqueio de arquivos por extensão, Mime Type, nome e hash;

2.6.26. Deverá permitir análise de arquivos comprimidos e protegidos por senha;

2.6.27. Deverá permitir criação de políticas por IP, domínio, grupo ou usuário;

2.6.28. Deverá permitir listas de bloqueio e liberação por IP, hostname e campo FROM;

2.6.29. Deverá monitorar URLs em mensagens, reescrevendo ou bloqueando links maliciosos, aplicando sandbox ou isolamento de navegador quando necessário;

2.6.30. Deverá registrar logs detalhados com nome do arquivo, hash, usuário afetado e método de detecção;

2.6.31. O console de administração deverá ser centralizado, em nuvem,

acessível via navegador (Google Chrome ou equivalente), com criptografia e autenticação multifator;

2.6.32. Deverá permitir definição de perfis de acesso e auditoria completa das ações;

2.6.33. Deverá suportar integração com Active Directory via LDAP/LDAPS e Azure AD via API;

2.6.34. Deverá registrar todas as atividades de usuários e administradores em logs de auditoria;

2.6.35. O console deverá fornecer visão consolidada de incidentes, estatísticas de e-mails e ameaças identificadas;

2.6.36. Deverá permitir rastreamento de mensagens (message tracking) por remetente, destinatário, assunto, data/hora, domínio e IP;

2.6.37. Deverá disponibilizar relatórios e consultas API REST, exportáveis em HTML e CSV;

2.6.38. Deverá permitir geração de alertas automáticos para detecção de malwares e phishing;

2.6.39. Deverá apresentar painel gerencial com indicadores de volume, classificação e origem das mensagens;

2.6.40. Deverá exibir informações geográficas sobre a origem de e-mails maliciosos.

## 2.7. REQUISITOS TÉCNICOS PARA AQUISIÇÃO DE SOLUÇÃO DE PROTEÇÃO AVANÇADA PARA ÁREAS DE ARMAZENAMENTO EM NUVEM (FILE SECURITY)

2.7.1. A solução deverá ser entregue na modalidade SaaS (Software as a Service);

2.7.2. A solução deverá possuir capacidade de escanear arquivos em áreas de armazenamento em nuvem (cloud storage);

2.7.3. A solução deverá identificar malwares, incluindo vírus, cavalos de troia, spyware e outros tipos de códigos maliciosos;

2.7.4. A solução deverá escanear os arquivos independentemente do tipo, tamanho ou extensão;

2.7.5. O tempo médio de escaneamento deverá ser inferior a 30 (trinta) segundos por arquivo;

2.7.6. A solução deverá ser escalável, com capacidade de realizar múltiplos escaneamentos simultaneamente;

2.7.7. O processo de deploy deverá ser realizado de forma padronizada, utilizando templates fornecidos pelo fabricante;

2.7.8. A solução deverá suportar, no mínimo, o serviço Amazon Simple Storage Service (S3);

2.7.9. A solução deverá identificar arquivos maliciosos por meio de múltiplas camadas de detecção, incluindo:

- Reputação, através da rede global de ameaças do fabricante;
- Proteção de variantes para identificar malwares modificados por algoritmos polimórficos ou técnicas de ofuscação;

2.7.10. A solução deverá permitir integração com o fluxo de trabalho do cliente, de forma a identificar arquivos maliciosos no momento do upload;

2.7.11. A arquitetura da solução deverá permitir a criação de buckets ou áreas de quarentena dedicadas para arquivos maliciosos identificados durante o escaneamento;

2.7.12. A solução deverá permitir a identificação do resultado do escaneamento por meio de tags aplicáveis aos arquivos, para uso e automação nos fluxos de trabalho;

2.7.13. A solução deverá suportar o escaneamento de, no mínimo, os seguintes tipos de arquivos: BIN, EXE, JPEG, MP4, PDF, TXT e ZIP;

2.7.14. A solução deverá ser operável tanto a partir de uma console gráfica quanto via API;

2.7.15. A documentação pública de API deverá estar disponível no site do fabricante e acessível por meio da console de gerenciamento;

2.7.16. A solução deverá possibilitar a integração com ferramentas de automação, pipelines de CI/CD ou sistemas de controle de versão em nuvem, permitindo inspeção de arquivos antes da publicação;

2.7.17. A solução deverá possuir arquitetura compatível com ambientes híbridos e multicloud, suportando integração com provedores de armazenamento adicionais além do Amazon S3;

2.7.18. A solução deverá prover relatórios detalhados de detecções, contendo data, hora, tipo de ameaça, nome do arquivo, hash, resultado do escaneamento e ação tomada;

2.7.19. A solução deverá permitir a geração de logs auditáveis para integração com sistemas SIEM, utilizando protocolos padrão de mercado (como Syslog);

2.7.20. A solução deverá permitir o agendamento de escaneamentos automáticos conforme políticas de segurança da organização;

2.7.21. Deverá possibilitar configuração de políticas de quarentena automatizadas, baseadas em níveis de risco e tipo de ameaça detectada;

2.7.22. Deverá manter histórico de escaneamentos e registros de incidentes de segurança por, no mínimo, 30 (trinta) dias;

2.7.23. A solução deverá suportar APIs RESTful para integração com ferramentas de orquestração e automação de segurança (SOAR);

2.7.24. Deverá ser compatível com mecanismos de autenticação segura, como SAML, OAuth 2.0 e chaves de API;

2.7.25. Deverá fornecer console centralizada baseada em nuvem, com autenticação multifator e criptografia TLS nas comunicações;

2.7.26. Deverá permitir a criação de perfis de acesso distintos para administradores, operadores e auditores;

2.7.27. Deverá permitir a exportação dos relatórios de detecção nos formatos CSV, JSON e PDF;

2.7.28. A solução deverá permitir a configuração de notificações automáticas via e-mail ou webhook para alertas de arquivos maliciosos

detectados;

2.7.29. A solução deverá utilizar base de reputação atualizada continuamente pela rede de inteligência de ameaças do fabricante;

2.7.30. A solução deverá permitir atualização automática dos motores de detecção e algoritmos de verificação;

2.7.31. Deverá prover métricas de desempenho e auditoria em painel visual integrado à console de gerenciamento;

2.7.32. Deverá possuir integração nativa com a plataforma de detecção e resposta estendida (XDR) do mesmo fabricante;

2.7.33. Deverá suportar o isolamento automático de arquivos considerados suspeitos, mantendo sua cópia para análise posterior;

2.7.34. Deverá permitir integração com serviços de armazenamento de terceiros para quarentena, desde que certificados pelo fabricante;

2.7.35. A solução deverá possuir suporte técnico e documentação completa em língua portuguesa, com portal de suporte e base de conhecimento acessível 24x7.

## 3. Disposições Gerais Serviço

3.1. Suporte Premium.

3.1.1. Escopo de trabalho do Gerente de Relacionamento – Regime Híbrido – Departamentos Senac relacionados.

3.1.2. O Profissional, tem como objetivo trazer à contratante, uma visão estratégica no serviço de pós-venda das soluções TrendMicro, com o fornecimento de uma operação de especialistas de segurança no apoio e disponibilidade das atividades listadas abaixo, dente elas, segurança das informações e a conformidade com as normas e políticas estabelecidas. Maiores detalhes sobre as atribuições e suas características, listadas a seguir:

- Compreender as necessidades e expectativas dos clientes internos e externos em relação à segurança da informação, bem como os riscos e ameaças envolvidos.
- Definir, implementar e monitorar os planos de ação para mitigar os riscos e garantir a segurança dos dados, sistemas e

infraestrutura de TI relacionado à solução TrendMicro.

- Estabelecer e manter uma comunicação efetiva com as áreas de negócio, TI e segurança, buscando alinhar as estratégias, objetivos e prioridades.
- Promover a conscientização e a educação sobre a importância da segurança da informação, disseminando as boas práticas e orientando os usuários sobre o uso adequado dos recursos de TI.
- Avaliar e recomendar soluções de segurança adequadas às necessidades da organização, considerando os aspectos técnicos e legais.
- Gerenciar os incidentes de segurança, coordenando as equipes envolvidas, reportando os resultados e providenciando as medidas corretivas e preventivas.
- Acompanhar as tendências e as novidades em segurança da informação, buscando atualizar seus conhecimentos e identificar oportunidades de melhoria relacionado à solução TrendMicro com um perfil "advisor".
- É o ponto único de contato para escalações com disponibilidade 24x7, para casos de severidade 1, envolvendo a operação de especialistas para uma análise troubleshooting aprofundado;
- Fará apresentações de Reports Técnicos, Reuniões Periódicas e Workshops;
- Otimizar a produtividade da área de TI e da empresa como um todo
- Aperfeiçoar processos e infraestrutura
- Priorizar a colaboração entre equipes e sistemas
- Integrar os frameworks de TI aos processos de gerenciamento de serviços
- Atualizar-se no mundo digital de forma assertiva, prática e coerenteDesenvolverá a entrega de Relatórios.
- Disponibilidade – O Gerente de Relacionamento poderá ser contatado através de seu telefone celular e e-mail que serão disponibilizados aos clientes em seu primeiro contato, denominado no Suporte Premium de Reunião de Kick-off. Ele estará disponível 24x7 para incidentes Severidade 1, garantindo o engajamento e orquestração da operação de especialistas de segurança da Contratada. Atuará de forma híbrida e quando necessário as agendas presenciais ocorrerão na regional Senac SP – Sede
- Gestão de casos de suporte técnico – O Gerente de Relacionamento será sempre acionado de forma automática, através de uma ligação ou um e-mail informando que a contratante realizou a abertura de um chamado de severidade crítica. Ele deverá atuar para que o atendimento esteja dentro

dos SLAs acordados, quando necessário a orquestração de "War Room" para troubleshooting e identificação da causa raiz do problema.

- Relatório Técnico de Negócios - O Gerente de Relacionamento mensalmente e trimestralmente deverá emitir a contratada um Relatório Técnico de Negócios, contendo todas as informações de utilização do serviço durante o período. São dados como: casos de suporte, severidades, tempos de resposta, atividades proativas desenvolvidas, ações de melhorias e recomendações.
- Visão Global de Proteção - O Gerente de Relacionamento, deverá realizar o Protection Overview da solução do TrendVision ONE através dos especialistas que compõem essa operação. Esse relatório é baseado nas melhores práticas do fabricante, um Health Check da ferramenta dentro do ambiente do Senac.
- Escalação de casos de suporte - O Gerente de Relacionamento deverá possuir recursos e contatos internos para acionamento, se for notado que o caso de suporte não está evoluindo para um cenário de resolução no tempo que atenda os acordos de SLA. A escalação dos casos será julgada pelo profissional em conjunto com sua liderança para que se garanta que todos os passos solicitados por nossos times técnicos foram seguidos, mas sem efeitos necessários para um cenário resolutivo.

3.1.3. Escopo de Trabalho do Consultor Técnico Dedicado Presencial – Regional Senac SP;

3.1.4. O Serviço do Consultor Técnico Dedicado requer acesso a níveis de conhecimentos especializados para ajudar a maximizar a postura de segurança, evitar eventos adversos e minimizar as consequências em caso de incidentes. O profissional deve oferecer o mais alto nível de suporte operacional da TrendMicro, implementar melhores práticas e suporte do produto TrendMIcro VisionOne. Será responsável pelas atividades proativas (health-checks, assessments, policy review) e apoiar no processo de troubleshooting dasolução. Escopo de Atividades:

- Apoio ao processo de Troubleshooting do Suporte Técnico TrendMicro;
- 8x5, durante o horário comercial;
- Fora do horário comercial (somente chamados de Severidade 1);
- A Monitoramento contínuo: Acompanhamento proativo da infraestrutura do cliente para garantir que a solução esteja funcionando corretamente e detectando possíveis incidentes ou ameaças.

- Alertas e notificações: Configuração e ajuste de alertas personalizados conforme o perfil e as necessidades do SENAC, para que possíveis problemas sejam identificados rapidamente.
- Análise de desempenho: Monitoramento do desempenho da solução para assegurar que os recursos estejam sendo utilizados de forma otimizada, com ajustes quando necessário.
- Apoio técnico especializado: Atendimento a chamados e tickets de suporte técnico, oferecendo assistência imediata na resolução de problemas ou incidentes relacionados ao Trend Micro Vision One.
- Resolução de falhas e bugs: Diagnóstico e solução de falhas ou problemas no sistema, buscando minimizar impactos na operação do cliente.
- Gestão de incidentes críticos: Atendimento prioritário e rápido para incidentes de segurança, como ameaças avançadas ou falhas que possam comprometer a proteção dos dados e sistemas do cliente.
- Análise detalhada de logs: Aprofundamento na análise de logs de segurança para detectar padrões anômalos, ameaças emergentes ou possíveis falhas de configuração.
- Geração de relatórios personalizados: Criação de relatórios de segurança detalhados para o cliente, com insights sobre incidentes, status da proteção e recomendações de melhorias.
- Atualizações automáticas e manuais: Suporte na configuração e aplicação de atualizações automáticas ou manuais para garantir que a solução esteja sempre protegida contra as ameaças mais recentes.
- Notificação de patches críticos: Comunicação proativa com o cliente sobre a necessidade de atualização de versões ou patches de segurança urgentes.
- Testes de compatibilidade: Auxílio na verificação de compatibilidade das atualizações com a infraestrutura do cliente, evitando problemas após a implementação.
- Consultoria de segurança: Fornecimento de recomendações sobre como melhorar a postura de segurança do cliente, com base nas melhores práticas e nas vulnerabilidades identificadas.
- Consultoria contínua: Assistência no planejamento de segurança a longo prazo, garantindo que a infraestrutura do cliente evolua de forma segura, com base nas novas ameaças e tendências de segurança.
- Integração com SIEM (Security Information and Event Management): Auxílio na integração do Trend Micro Vision One com outras soluções de segurança (SIEM, antivírus, firewalls, etc.) para uma visibilidade centralizada e melhor resposta a

incidentes.

- Conectividade com APIs e ferramentas externas: Suporte técnico para configurar integrações com outras ferramentas e plataformas do cliente, como soluções de monitoramento de rede, proteção de endpoint, etc.
- Avaliação constante de ameaças e vulnerabilidades: Análise contínua de novos tipos de ameaças cibernéticas para ajustar e melhorar as configurações e defesas da solução.
- Recomendações para melhorar a postura de segurança: Fornecimento de sugestões sobre como aprimorar continuamente a estratégia de segurança do cliente, incluindo ajustes nas configurações do Trend Micro Vision One.
- Apoio com dúvidas em geral e HOWTOs;
- Atividades Proativas:
- Architecture Design & Review: Desenho e revisão da arquitetura (PréProjeto & Pós-Projeto);
- Upgrade Assistance: atualização da solução para versões mais recentes;
- Maturity Assessment: Recomendação de melhores prática da solução (Processos e Configurações);
- ToI (Transfer of Information): Transferência de conhecimento da solução com base em Hands-On & Workshops;
- Health-Check: avaliação da saúde e capacidade do ambiente;
- Proof of Concept: elaboração de provas de conceito e apoio ao processo de homologação de pilotos;
- Deployment Assistance: apoio no processo de instalação de um novo ambiente;
- Integration Assistance: apoio na integração de produtos Product Policy Advisory: apoio ao processo de elaboração de políticas;
- Security Program Review: avaliação do nível de proteção da Segurança da Informação (agnóstico);

3.1.5. Relatório Mensal de Incidentes e Atividades Proativas;

3.1.6. Premissas:

- A Contratante deverá acompanhar a atividade integralmente para fornecimento de informações pertinentes ao mesmo;
- A Contratada deverá fornecer e relacionar os incidentes através de uma solução Centralizadora de logs (sem ônus para a Contratante) ou Solução da própria fabricante.
- A Contratante deverá prover todo o recurso e acesso necessário que sejam imprescindíveis para a execução das atividades contempladas no escopo do serviço;

- Todo o hardware e software necessários para a conectividade/comunicação da solução Trendmicro serão solicitados à contratante previamente conforme o dimensionamento inicial para suportar as estações/servidores com o client endpoint.

3.1.7. As atividades previstas para os temas: Suporte Premium para o ambiente TrendMicro: Consultor Técnico estão direcionadas para a regional Senac SP - Sede.

3.1.8. Todas as atividades que envolvam ações junto à estação de trabalho do usuário, são de responsabilidade da equipe de trabalho do Senac, restando a Contratada apenas a formulação de procedimentos operacionais;

3.1.9. Para atividades que podem ser entregues remotamente, a Contratada fornecerá uma solução de sessão remota;

3.1.10. É de responsabilidade do Senac ter uma ferramenta ou utilizar um próprio método para realizar a distribuição de soluções de Endpoint (agentes), cabendo a Contratada, realizar o acompanhamento do processo e dos testes/homologação com o usuário final;

3.1.11. Horário de Trabalho

- O número de horas para cada tarefa será distribuído ao longo da semana, sendo no máximo oito (08) horas de trabalho em cada dia. O horário de início de trabalho será determinado pelo Serviço Nacional de Aprendizagem Comercial - SENAC, para cada um dos sites envolvidos no projeto, respeitados os limites do horário comercial (segunda a sexta-**feira** das 08h00min às 18h00min, exceto feriados) com uma hora de almoço.
- As atividades definidas no escopo serão executadas remotamente em cada site ou presencialmente caso seja acordado, desde que, as atividades eventuais on-site (com exceção às relacionadas dos perfis direcionados à regional Senac SP – Sede), seu deslocamento para as demais regionais será custeado pela Contratante da respectiva regional solicitante.

3.1.12. Características do Suporte 24x7 – SOC -Time Remoto - Escopo do Suporte:

- A modalidade de suporte que está sendo considerada nesta proposta é de gestão remota da solução 24x7x365 por parte da Contratada. Fica a cargo da Contratada todas as atividades de

rotina e gestão da ferramenta, tais como extração de relatórios, atualizações, instalação e remoção de agentes dentre outras de maior criticidade e segurança.

- Neste documento, estão sendo considerados cobertos pelo suporte os produtos abaixo:
- Trend Vision One - Endpoint Security (Pro).
- Trend Vision One - Endpoint Security (Essentials).
- Trend Vision One Attack Surface Risk Management.
- TrendMicro Mobile Security
- TrendMicro VisionOne Email and Collaboration Security
- TrendMicro VisionOne File Security

3.1.13. Metodologia de Atendimento;

3.1.14. Os SLAs serão atendidos conforme criticidade dos mesmos e do Serviço Nacional de Aprendizagem Comercial - SENAC, desde questionamentos quanto à instalação, configuração e utilização dos produtos até resolução de problemas críticos, dentro dos seguintes formatos e time:

3.1.15. Equipe Blueteam / monitoração ativa composta de mínimo 6 pessoas compondo a equipe, com perfis multidisciplinares, como:

- Analista de vulnerabilidades;
- Analista de monitoramento;
- Analista de resposta a incidentes;
- Equipe de atendimento Atendimento Eletrônico
- Monitoramento contínuo: Acompanhamento proativo da infraestrutura do cliente para garantir que a solução esteja funcionando corretamente e detectando possíveis incidentes ou ameaças.
- Alertas e notificações: Configuração e ajuste de alertas personalizados conforme o perfil e as necessidades do SENAC, para que possíveis problemas sejam identificados rapidamente.
- Análise de desempenho: Monitoramento do desempenho da solução para assegurar que os recursos estejam sendo utilizados de forma otimizada, com ajustes quando necessário.
- Apoio técnico especializado: Atendimento a chamados e tickets de suporte técnico, oferecendo assistência imediata na resolução de problemas ou incidentes relacionados ao Trend Micro Vision One.
- Resolução de falhas e bugs: Diagnóstico e solução de falhas ou problemas no sistema, buscando minimizar impactos na operação do cliente.
- Gestão de incidentes críticos: Atendimento prioritário e rápido para incidentes de segurança, como ameaças avançadas ou

falhas que possam comprometer a proteção dos dados e sistemas do cliente.

- Análise detalhada de logs: Aprofundamento na análise de logs de segurança para detectar padrões anômalos, ameaças emergentes ou possíveis falhas de configuração.
- Geração de relatórios personalizados: Criação de relatórios de segurança detalhados para o cliente, com insights sobre incidentes, status da proteção e recomendações de melhorias.
- Atualizações automáticas e manuais: Suporte na configuração e aplicação de atualizações automáticas ou manuais para garantir que a solução esteja sempre protegida contra as ameaças mais recentes.
- Notificação de patches críticos: Comunicação proativa com o cliente sobre a necessidade de atualização de versões ou patches de segurança urgentes.
- Testes de compatibilidade: Auxílio na verificação de compatibilidade das atualizações com a infraestrutura do cliente, evitando problemas após a implementação.
- Consultoria de segurança: Fornecimento de recomendações sobre como melhorar a postura de segurança do cliente, com base nas melhores práticas e nas vulnerabilidades identificadas.
- Consultoria contínua: Assistência no planejamento de segurança a longo prazo, garantindo que a infraestrutura do cliente evolua de forma segura, com base nas novas ameaças e tendências de segurança.
- Integração com SIEM (Security Information and Event Management): Auxílio na integração do Trend Micro Vision One com outras soluções de segurança (SIEM, antivírus, firewalls, etc.) para uma visibilidade centralizada e melhor resposta a incidentes.
- Conectividade com APIs e ferramentas externas: Suporte técnico para configurar integrações com outras ferramentas e plataformas do cliente, como soluções de monitoramento de rede, proteção de endpoint, etc.
- Avaliação constante de ameaças e vulnerabilidades: Análise contínua de novos tipos de ameaças cibernéticas para ajustar e melhorar as configurações e defesas da solução.
- Recomendações para melhorar a postura de segurança: Fornecimento de sugestões sobre como aprimorar continuamente a estratégia de segurança do cliente, incluindo ajustes nas configurações do Trend Micro Vision One.
- Email - Destina-se a solução de questionamentos e/ou problemas que não necessitam de solução imediata, assim como detalhamento de sugestões de melhoria da solução. Os

e-mails serão analisados e uma resposta será enviada de acordo com a criticidade.

- Atendimento Telefônico: Destina-se a solução de questionamentos e/ou problemas que necessitem de solução imediata. A troca rápida de informações transmite segurança e conforto ao usuário na operação do sistema.
- Acesso Remoto: Em caso de algum problema ou questão persistir, mesmo após o atendimento Eletrônico ou Telefônico, deverá ser solicitado ao Serviço Nacional de Aprendizagem Comercial - SENAC autorização para conexão remota a fim de sanar a ocorrência.
- Microsoft Teams: Para troca de informações rápidas e imediatas será disponibilizado um grupo do Teams para internação do fornecedor e a Equipe técnica do Senac.

3.1.16. SLA – Service Level Agrrement;

3.1.17. Devido à criticidade dos sistemas adquiridos pelo Serviço Nacional de Aprendizagem Comercial - SENAC, a Contratada estabelece, em acordo com o Senac, um nível de serviço que atenda às necessidades e forneça subsídios para priorização no atendimento. Este serviço é constituído por um sistema onde o fator Severidade define o tempo e nível de atendimento, descrito em mais detalhes abaixo:

- A abertura dos chamados se dará por parte do Serviço Nacional de Aprendizagem Comercial - SENAC.

| Severidade | Impacto ao Negócio | SLA de Resposta |
|---|---|---|
| 1 | Solução Indisponível | Em até 1 hora após abertura do chamado |
| 2 | Produção Impactada | Em até 2 horas após abertura do chamado |
| 3 | Componente Impactada | Em até 6 horas após abertura do chamado |
| 4 | Problema de menos impacto dúvidas e Documentações | Próximo dia útil, horário comercial após a abertura do chamado. |

- No momento da abertura do chamado, o nível de severidade será identificado pela equipe da Contratada, de acordo com o grau de seu impacto. A Contratada poderá alterar a severidade, se esta alteração se fizer necessária, para atender os Níveis de Serviços Acordados.

3.1.18. Relatório Mensal:

- Para que o Serviço Nacional de Aprendizagem Comercial - SENAC possa manter- se informado de todos os aspectos, a Contratada deverá enviar mensalmente um relatório executivo. Este relatório deverá conter dados importantes, que irão agregar valor e fornecer parâmetros para tarefas e decisões a serem tomadas referentes à solução contratada. Neste relatório, deverão conter as seguintes informações:
- Panorama de Segurança: um resumo dos eventos mais importantes, ameaças descobertas e informações do mercado de segurança durante o mês, e os comentários da equipe da Contratada.
- Informações sobre a solução: as novidades, atualizações e informações referentes à solução contratada. Neste aspecto, a Contratada informará sobre os releases que podem auxiliar na utilização e por fim diretamente no negócio do Serviço Nacional de Aprendizagem Comercial - SENAC.
- Chamados do mês: A descrição detalhada dos chamados solicitados, seu status e resolução. Contempla também um sumário destacando as informações referentes ao SLA contratado.
- Informações geradas pelo monitoramento: Performance, Disponibilidade, Latência, e outras informações específicas de cada solução; Resultado da verificação de registros e as ações e procedimentos executados: Caso sejam necessários; Resultado da verificação das políticas e configurações: Com as ações e procedimentos executados, caso necessário.
- Workshop Trimestral a Contratada deverá realizar trimestralmente um Workshop para divulgação de Melhores Práticas, Features, Novas Tecnologias e Tendências relacionadas ao software TrendMicro Vision ONE, que será realizado no Serviço Nacional de Aprendizagem Comercial - SENAC site São Paulo, com a participação das demais localidades ou remotamente conforme acordado.

3.1.19. Modalidade de Suporte Reativo:

- O suporte reativo, consiste no acionamento da equipe de suporte, com o registro de chamados por parte da equipe Serviço Nacional de Aprendizagem Comercial - SENAC.
- O atendimento se dará na forma de contato telefônico e acesso remoto a ser liberado pelo time SENAC, conforme localidade assistida por este serviço. Atividades de saneamento de dúvidas, procedimentos de instalação, remoção, alteração, configuração de políticas, aplicação de

patches, upgrade da solução.

3.1.20. Suporte Proativo:

- O suporte proativo, consiste na detecção de falhas e abertura de chamados por parte da equipe técnica da Contratada. Todas as atividades de monitoração do ambiente e detecção de falhas deverão ser detectadas pelo time de suporte da Contratada.
- O suporte proativo deverá ser na modalidade 24x7. Os chamados abertos dentro ou fora do horário comercial poderão ser abertos por E-mail, Portal do Usuário e Telefone. O SLA só começará a ser contado a partir da abertura do chamado.
- Para esta modalidade de atendimento com o suporte proativo, será disponibilizado por parte do Senac os seguintes acessos:
- Liberação de acesso ao ambiente TrendMicro;
- Liberação de regras de firewall para acesso externo ao servidor da solução;
- Liberação de acesso no modelo VPN (Virtual Provider Networking), acesso seguro e criptografado.

3.1.21. Implementação e Configuração:

- Implementação da plataforma seguindo as melhores práticas do fabricante.
- Apoio de instalação de a gente em caso de falha, para análise de log em caso de erro de instalação.
- Apoio em sessão remota para avanço de instalação de agente.
- Abertura de chamado com o fabricante em caso de erro de instalação.
- Validação de agentes reportados ao console de gerenciamento.
- Configuração das políticas de segurança seguindo as melhores práticas do fabricante.

3.1.22. Treinamento Oficial:

- Acesso a plataforma de treinamentos oficiais da ferramenta.

## 4. DESCRIÇÃO PROPOSTA DE SERVIÇO

4.1. Serviços de Suporte Premium para o ambiente TrendMicro com Gerente de Relacionamento de Segurança e Consultor Técnico Dedicado com a necessidade de atendimento personalizado no ambiente de TI, o Serviço Nacional de Aprendizagem Comercial – SENAC tem como objetivo a

contratação da gestão do ambiente de proteção de endpoints TrendMicro VisionOne e atendimento Premier com análise de vulnerabilidade, relatório de saúde do ambiente e revisões proativas do ambiente para melhoria contínua e suporte na modalidade 24x7x365.

Considerando o seguinte cenário:

| Estado | SOC | Suporte | Qtd Endpoint | Qtd Servidor | ASMR | Mobile | Email Collaboration | File Security | Tenant |
|---|---|---|---|---|---|---|---|---|---|
| Acre | 1 | 1 | 139 | 12 | | | | | 2 |
| Amazonas | | | 53 | 21 | | | | | 2 |
| Amapá | | | 398 | 6 | | | | | 2 |
| Brasília | | | 1948 | 1 | | | | | 2 |
| Espírito Santo | | | 1500 | 41 | 1477 | | | | 2 |
| Maranhão | | | 238 | 1 | | | | | 2 |
| Rio Grande do Norte | | | 0 | 60 | | | | | 2 |
| Rondônia | | | 92 | 4 | | | 1241 | | 2 |
| Roraima | | | 90 | 15 | | | | | 2 |
| Santa Catarina | | | 129 | 49 | | | | | 2 |
| São Paulo | | | 25520 | 1550 | 1550 | 100 | | 2 | 3 |
| Tocantins | | | 150 | 25 | | | | | 2 |
| Pará | | | 250 | 55 | | | | | 2 |
| **Total** | **1** | **1** | **30.507** | **1840** | **3027** | **100** | **1241** | **2** | **27** |

## 5. Prazo de Entrega

5.1 As licenças deverão estar disponíveis por e-mail, ou site do Fabricante para visualização e uso, em até 5 dias úteis a partir do recebimento do Acordo de Compra, e as licenças deverão ser nominais ao Senac São Paulo.

## 6. Remuneração

6.1. O pagamento será realizado em única vez diretamente à Contratada em até 28 (vinte e oito) dias após recebimento do acordo de compra, através de emissão de nota fiscal e boleto bancário.

6.2. O **Fornecedor** deverá apresentar ao **Senac** a nota fiscal no prazo de 15 (quinze) dias antes do vencimento, visando ao atendimento da legislação aplicável em vigor.

**Gerência de Materiais e Serviços**
**Senac São Paulo**

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
E-mail: licitacao.gms@sp.senac.br
www.sp.senac.br

6.3. A não efetivação do pagamento na forma e no prazo estabelecidos no presente Termo de Referência implicará na incidência de multa de 2% (dois por cento) do valor devido. Se o atraso for superior a 30 (trinta) dias, incidirão também juros de 6% (seis por cento) ao ano, calculados "pro-rata-mês", bem como atualização monetária pelo IGP-M/FGV calculada "pro-rata-die" até a data de seu efetivo pagamento.

6.4. O **Senac** poderá reter o(s) pagamento(s) previsto(s) na proposta comercial nas seguintes hipóteses:

6.4.1. se **o Fornecedor** não encaminhar as notas fiscais para o endereço correto e em tempo hábil;

6.4.2. se **o Fornecedor** deixar de apresentar os documentos exigidos neste processo ou nele sejam constatadas quaisquer irregularidades;

6.4.3. se houver erro de faturamento ou divergência de valor;

6.4.4. se **o Fornecedor** fornecer Serviços irregulares;

6.4.5. para cobrir as obrigações previdenciárias e trabalhistas incidentes na execução dos Serviços e/ou em eventuais Reclamações Trabalhistas; ou

6.4.6. se existirem pendências de responsabilidade do **Fornecedor**.

6.5. O valor homologado permanecerá inalterado pelo prazo de 12 (doze) meses contados da assinatura do presente Contrato, podendo ser reajustado após esse prazo, mediante solicitação do Fornecedor, pelo percentual da variação acumulada do IPCA apurado no período.

6.6. O índice fixado para o reajuste será o mesmo para toda a vigência, salvo se ocorrer a sua extinção, quando então as Partes poderão acordar outro índice para substituí-lo.

6.7. Será considerado para a concessão do reajuste o período dos últimos 12 (doze) meses anteriores ao mês de solicitação do reajuste feita pelo **Fornecedor**.

6.8. O valor homologado poderá ser revisto a qualquer tempo caso uma das Partes, considerando-se prejudicada, comprove inequívoco desequilíbrio econômico-financeiro que torne inviável a relação contratual.

6.9. Todos os encargos sociais, fiscais, trabalhistas, previdenciários e de acidente do trabalho correrão por conta do **Fornecedor**, nenhuma responsabilidade cabendo ao **Senac**.

6.10. Eventuais retenções na fonte de referidos encargos serão realizadas pelo **Senac**, na forma da legislação em vigor.

6.11. Estão incluídas no valor do presente Acordo de Compra todas as despesas decorrentes da execução dos Serviços.

## 7. Vigência

7.1. A vigência será de 12 (doze) meses, a partir do recebimento do Acordo de Compra, podendo:

7.1.1. sua vigência ser prorrogada automaticamente, caso não haja manifestação em contrário de quaisquer das Partes com antecedência mínima de 30 (trinta) dias, até o limite máximo de 60 (sessenta) meses, ou

7.1.2. ser denunciado pelas Partes, por escrito, a qualquer momento, com antecedência mínima de 30 (trinta) dias, ressalvando-se que, em até 2 (dois) úteis contados da data da comunicação escrita da denúncia, o **Fornecedor** procederá à devolução ao **Senac** do valor dos Serviços que ainda não tiverem sido executados se o **Senac** já tiver efetuado o pagamento.

7.2. O Contrato será considerado rescindido pelo **Senac**, de pleno direito, sem aviso prévio:

7.2.1. se a outra Parte entrar em liquidação voluntária ou compulsória, tornar-se insolvente ou falida ou requerer/for requerida sua insolvência, recuperação judicial ou extrajudicial ou falência e/ou for impedida/proibida de exercer suas atividades; ou

7.2.2. por motivo de força maior ou caso fortuito, na medida em que impossibilite total ou parcialmente o cumprimento das obrigações assumidas neste termo, ficando o **Senac** liberado do pagamento dos Serviços não executados.

7.3. O Fornecedor não poderá ceder ou transferir, parcial ou totalmente, as obrigações assumidas no presente processo sem a prévia e expressa autorização, por escrito, do Senac. Concedida referida autorização, o Fornecedor continuará responsável pelos Serviços contratados.

7.4. A sucessão contratual será permitida somente em decorrência de operações societárias de fusão, cisão ou incorporação realizada pelo **Fornecedor** e, desde que:

7.4.1. previamente analisada e consentida pelo **Senac**, considerando eventuais riscos ou prejuízos para o adimplemento contratual;

7.4.2. sejam mantidas todas as condições contratuais; e

7.4.3. exista expressa concordância do sucessor em assumir a responsabilidade pela execução do presente processo e receber os créditos dele decorrentes.

7.5. É vedada a cessão ou transferência parcial ou total de qualquer crédito, bem como a emissão, por parte do Fornecedor, de qualquer título de crédito decorrente do Acordo de Compra sem a prévia e expressa autorização, por escrito, do Senac.

## 8. Multa

8.1. Fica estipulada multa correspondente 10% (dez por cento) do valor anual do Contrato, sem prejuízo de indenização suplementar pelos danos comprovadamente causados, na qual incorrerá a parte que infringir quaisquer cláusulas deste termo, excetuada:

8.1.1. a hipótese de atraso no pagamento, para a qual a penalidade está prevista no **Item 6.3** deste Termo de Referência e;

8.1.2. eventuais penalidades específicas previstas em Anexos relacionadas a execução dos Serviços, não limitadas a Níveis Mínimos de Serviço e/ou avaliações, facultando-se, ainda, à Parte inocente o poder de considerar simultaneamente rescindido o presente instrumento, independentemente de qualquer notificação ou interpelação judicial ou extrajudicial.

8.2. Os termos e condições deste termo somente poderão ser alterados por meio de termo de aditamento escrito e:

8.2.1. de acordo com a vontade das Partes ou;

8.2.2. em caso de determinação ou nova regulamentação da Autoridade Nacional de Proteção de Dados ("ANPD") relativamente às cláusulas que regulam o tratamento de dados pessoais.

**ANEXO II**

**PREGÃO ELETRÔNICO Nº PEE 2025000116**

**MODELO DE PROPOSTA COMERCIAL**

| DESCRIÇÃO | QTD | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|
| Trend Vision One - Endpoint Security (Essentials) | 30507 | R$ | R$ |
| Trend Micro Workload Security - PRO | 1840 | R$ | R$ |
| Trend Vision One Attack Surface Risk Management | 3027 | R$ | R$ |
| Trend Micro Mobile Security | 100 | R$ | R$ |
| Trend Vision One Email and Collaboration Security | 1241 | R$ | R$ |
| Trend Vision One File Security per 500K | 2 | R$ | R$ |
| Serviços de Monitoramento Proativo 24x7 nos departamentos Regionais do Senac. Suporte, Implementação Atualização de produto Premium Trend Micro pelo período de 12 meses com Treinamento Oficial | 12 Meses | R$ | R$ |
| **VALOR TOTAL GLOBAL** | | | R$ |

**Obs.:**
**1)** Validade da Proposta: 90 (noventa) dias;
**2)** Condições de Pagamento: será realizado em única vez diretamente à Contratada em até 28 (vinte e oito) dias após recebimento do acordo de compra, através de emissão de nota fiscal e boleto bancário
**3)** Vigência: 12 (doze) meses, podendo ser prorrogado até o limite de 60 (sessenta) meses;
**4)** Dados da empresa que efetuará o faturamento:
Razão Social:.....
Endereço:.....Cep.....Bairro.....Município.....Estado.....
CNPJ .....
Inscrição Estadual .....
Contato.....Fone.....Fax.....
E-Mail .....

Localidade, dia, mês e ano.

Assinatura
(nome completo e cargo do representante legal da Empresa – somente sócios administradores / proprietários ou procuradores com poderes específicos).

**Gerência de Materiais e Serviços**
**Senac São Paulo**

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
E-mail: licitacao.gms@sp.senac.br
www.sp.senac.br

# ANEXO III

# PREGÃO ELETRÔNICO - PEE 2025000116

# TGC "TERMO GERAL DE CONTRATAÇÃO"

**Gerência de Materiais e Serviços**
**Senac São Paulo**

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
E-mail: licitacao.gms@sp.senac.br
www.sp.senac.br

**CONTRATO DE PRESTAÇÃO DE SERVIÇOS**
**Nº /20**

| **1. PARTES** | | |
|---|---|---|
| **CONTRATANTE** | **Serviço Nacional de Aprendizagem Comercial – Senac**, Administração Regional no Estado de São Paulo, inscrito no CNPJ sob nº 03.709.814/0001-98, com sede na Rua Dr. Vila Nova, 228, 7º andar, São Paulo, SP, CEP 01222-903, representado conforme indicado abaixo: | |
| | **Unidade/Gerência** | **Gerência de Tecnologia da Informação** |
| | **CNPJ** | 03.709.814/0001-98 |
| | **Endereço** | Rua Dr. Vila Nova, 228, 3° andar |
| | **Representante Legal** | Inserir nome completo do Representante Legal |
| | **CPF do Representante Legal** | Inserir CPF do Representante Legal |
| | **Cargo do Representante Legal** | Inserir cargo do Representante Legal |
| **CONTRATADA** | **Razão Social/ Nome/Nome Social** | **Inserir Razão Social ou Nome completo/Nome Social** |
| | **CNPJ/CPF** | Inserir CNPJ/CPF |
| | **Endereço** | Inserir endereço completo da Contratada |
| | **Representante(s) Legal(is)** | Inserir nome completo do(s) Representante(s) Legal(is) |
| | **CPF do(s) Representante(s) Legal(is)** | Inserir CPF do(s) Representante(s) Legal(is) |

1. As Partes acima qualificadas, doravante designadas "Partes" quando mencionadas em conjunto, e "Parte" quando mencionadas individualmente, resolvem firmar o presente Contrato de Prestação de Serviços ("**Contrato**"), mediante as cláusulas e condições estipuladas neste instrumento e em conformidade com o Regulamento de Licitações e Contratos do Senac vigente.

2. Integram o presente **Contrato**, no que lhe for aplicável, (i) os Anexos relacionados na Cláusula 7 e, independentemente de transcrição, (ii) o Termo Geral de Contratação do Senac São Paulo ("**TGC**") adotado pelo **Senac** para contratação de serviços e/ou aquisição de bens, devidamente registrado no 8º Oficial de Registro de Títulos e Documentos e Civil de Pessoa Jurídica da Comarca de São Paulo sob nº 1.591.854, que pode ser consultado e/ou obtido por meio do link bit.ly/45psxaM, e, (iii) em se tratando de contrato licitado, o respectivo Edital e seus Anexos referidos na Cláusula 3 abaixo.

**2. OBJETO (Cláusula 3 do TGC)**

Constitui objeto deste **Contrato** a prestação dos serviços **Aquisição das soluções trend micro para segurança da informação das estações de trabalho e servidores, com gestão centralizada e proteção para cargas de trabalho híbridas. Inclui gerenciamento de risco cibernético, identificação de exposição externa e detecção e resposta estendida para atender o Senac São Paulo e DRs participantes** ("Serviços") pela **Contratada**, conforme Anexos ao final relacionados, que integram o presente **Contrato** para todos os fins e efeitos de direito.

**3. TIPO DE CONTRATAÇÃO**

☒ Licitação - nº / **- exclusivo para licitação**
☐ Dispensa de Licitação
☐ Inexigibilidade de Licitação

| **4. VALOR, CONDIÇÕES, FORMAS/MEIOS DE PAGAMENTO, REAJUSTE E REPACTUAÇÃO** | |
|---|---|
| **VALOR DO CONTRATO (Cláusula 4 do TGC)** | ☐ R$ ( ) total<br>☐ R$ ( ) estimado |
| **CONDIÇÕES DE PAGAMENTO (Cláusula 4 do TGC)** | ☐ ( ) dias contados da apresentação da nota fiscal<br>☒ Conforme definido no Termo de Referência |

| | |
|---|---|
| **FORMAS DE PAGAMENTO (Cláusula 4 do TGC)** | ☐ Parcela única<br>☐ Mensal de R$ ( ) – todo dia ( )<br>☐ Equivalente ao somatório dos Serviços prestados dentro do mês, comprovados por meio de envio de relatório<br>☒ Conforme definido no Termo de Referência |
| **MEIOS DE PAGAMENTO (Cláusulas 4.1.2 e 4.1.3 do TGC)** | ☒ Boleto bancário<br>☐ Depósito em conta bancária de titularidade da **Contratada,** Banco , Agência , C/C nº |
| **REAJUSTE (Cláusula 5.1 do TGC)** | ☐ Não aplicável<br>☒ Sim. Índice: IPCA |
| **REPACTUAÇÃO – (Cláusula 5.3 do TGC) - exclusivo para licitação** | ☒ Não aplicável<br>☐ Sim. Categoria: |

| **5. VIGÊNCIA** | |
|---|---|
| **PRAZO DE VIGÊNCIA (Cláusula 6.1 do TGC)** | 12 (doze) meses, podendo ser renovado até 60 (sessenta) meses<br>**INÍCIO:** / /<br>**TÉRMINO:** / / |
| **PRAZO DE DENÚNCIA (Cláusula 6.2 do TGC)** | ☐ Não aplicável<br>☒ Com até 30 (trinta) dias de antecedência |
| **PERÍODO DA PRESTAÇÃO DOS SERVIÇOS - exclusivo para licitação** | **INÍCIO:** / /<br>**TÉRMINO:** / / |

| **6. CONDIÇÕES ESPECÍFICAS** | |
|---|---|
| **SERVIÇOS PRESTADOS DENTRO DAS DEPENDÊNCIAS DO SENAC (Cláusula 9 do TGC)** | ☒ Não aplicável<br>☐ Sim, Sindicato Data-base de cada ano |
| **GARANTIA CONTRATUAL - (Cláusula 9.4 do TGC) - exclusivo para licitação** | ☒ Não aplicável<br>☐ Sim, % ( por cento) do valor do **Contrato** |
| **DESPESAS (Cláusula 12 do TGC)** | ☒ Não haverá despesas<br>☐ Conforme definido no Termo de Referência |
| **DIREITOS AUTORAIS E PROPRIEDADE INTELECTUAL (Cláusula 13 do TGC)** | ☒ Não aplicável<br>☐ Aplicável |
| **USO DE IMAGEM, VOZ E/OU NOME (Cláusula 14 do TGC)** | ☒ Não aplicável<br>☐ Aplicável |
| **LGPD (Cláusula 17 do TGC)** | ☐ Controladores – Cláusula Simples (Cláusula 17.5.1 do **TGC**)<br>☐ Controladores – Cláusula Completa (Cláusula 17.5.2 do **TGC**)<br>☒ Controlador x Operador (Cláusula 17.5.3 do **TGC**) |
| **PENALIDADES (Cláusula 19 do TGC)** | ☒ Multa de ☐ R$ ( )<br>☒ 10% (dez por cento) sobre o valor anual do **Contrato** vigente à época da infração<br>☐ Além da multa assinalada acima, outras definidas no Termo de Referência |

| **7. ANEXOS** |
|---|
| Anexo I - Termo de Referência<br>Anexo II - Proposta datada de / /<br>Anexo III - Adendo ao Acordo de Tratamento de Dados Pessoais (Controlador x Operador) |

| **8. FORO (Cláusula 24 do TGC)** |
|---|

As Partes elegem o Foro da Comarca de **São Paulo** para solucionar litígios porventura decorrentes do **Contrato**, com expressa renúncia a qualquer outro, por mais privilegiado que seja.

As cláusulas e condições do **Contrato** passam a surtir efeitos a partir da data de emissão do presente instrumento.

E, por estarem justas e contratadas, as Partes assinam eletronicamente o presente **Contrato** e declaram e assumem o disposto na Cláusula 21.2 do **TGC**.

, de de 20 .

**Senac** **Contratada**