SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI
DEPARTAMENTO REGIONAL DE SÃO PAULO

CHAMAMENTO PÚBLICO

PROCESSO DE SELEÇÃO COM DISPUTA ABERTA

N.º 895/2025

AQUISIÇÃO DE PLATAFORMA DE SIMULAÇÃO DE ATAQUE E DEFESA CIBERNÉTICA HIPER-REALISTA AO SENAI-SP

DATA DA DISPUTA: 11/12/2025 ÀS 09H30 (HORÁRIO DE BRASÍLIA)

CRITÉRIO DE SELEÇÃO: ECONÔMICO (MENOR PREÇO)

GERÊNCIA DE COMPRAS

SUMÁRIO

PROCESSO DE SELEÇÃO COM DISPUTA
FORMA ABERTA - Nº 895/2025

1. NORMAS ESPECÍFICAS

1.1. O presente documento, denominado "Chamamento Público" poderá ser obtido por meio do *site* oficial do Serviço Nacional de Aprendizagem Industrial – SENAI: www.sp.senai.br, ou endereço eletrônico: https://transparencia.sp.senai.br/licitacoes-editais, ou plataforma eletrônica: https://licitacoes-e2.bb.com.br/aop-inter-estatico/, na qual ocorrerá a disputa de preços, sob o número 1084154.

1.2. As regras para processamento da disputa serão as mesmas utilizadas na referida plataforma, salvo disposto em contrário neste instrumento, diferenciando-se apenas no que diz respeito as terminologias.

1.3. As normas deste Chamamento Público serão interpretadas em favor da ampliação da disputa entre as participantes.

1.4. Este Processo de Seleção poderá ser justificadamente cancelado, no todo ou em parte, a qualquer momento, bem como, ter seus prazos prorrogados, a critério da Comissão de Contratação.

2. DO OBJETO

2.1. O presente Processo de Seleção tem por objetivo a aquisição de Plataforma de Simulação de Ataque e Defesa Cibernética Hiper-Realista, conforme Memorial Descritivo e demais anexos.

2.1.1. Critério de Seleção: Econômico – Menor Preço por Lote

2.1.2. Forma do Processo de Seleção: Com Disputa Aberta

2.1.3. Vigência Contratual: 12 meses, prorrogáveis por até 36 (trinta e seis) meses, nos termos dos artigos 34 e 38 do RCA.

2.2. O Processo de Seleção será regido pelo Regulamento para Contratação e Alienação – RCA do Serviço Nacional de Aprendizagem Industrial – SENAI por meio da Resolução CN-SENAI nº 14/2023, de 16/05/2023, devidamente publicado no Portal da Transparência do SENAI e pelas Normas Específicas contidas nesse Chamamento Público e nos seguintes anexos:

Anexo A	Modelo de Declaração sobre o Emprego de Menor e Outras Informações
Anexo B	Memorial Descritivo
	Anexo I – Termo de Referência
	Anexo II – Requisitos de Segurança e Privacidade
	Anexo III – Checklist – Requisitos de Segurança da Informação / Requisitos de Privacidade e Conformidade LGPD
Anexo C	Modelo de Proposta

Anexo D	Minuta de Contrato
Anexo E	Termo de Confidencialidade

2.3. **Definições**

2.3.1. Contratante: Serviço Nacional de Aprendizagem Industrial – SENAI, Departamento Regional de São Paulo.

2.3.2. Comissão de Contratação: formada por 3 membros, cuja atribuição é analisar, emitir pareceres técnico-financeiros, decidir acerca da qualificação dos participantes e das propostas, dos pedidos de reconsideração e do resultado do Processo de Seleção.

2.3.3. Condutor: um integrante da Comissão de Contratação que será o responsável pela condução da reunião de disputa, bem como das demais fases do processo.

2.3.4. Participante: empresa que apresentar proposta para o Processo de Seleção.

2.3.5. Contratada: empresa selecionada no Processo de Seleção.

3. DA PARTICIPAÇÃO

3.1. Poderão participar deste Processo de Seleção, empresas com ramo de atividade compatível com o objeto, comprovado por meio da Classificação Nacional de Atividade Econômica (CNAE), tal comprovação também poderá ser realizada por meio do Contrato Social.

3.2. Não poderão participar, empresas:

3.2.1. Reunidas sob regime de Consórcio;

3.2.2. Que possuam em seu quadro societário dirigente ou empregado do SENAI;

3.2.3. Suspensas temporariamente do direito de contratar com o SESI e o SENAI e as demais Entidades que integram o Sistema Indústria;

3.2.4. Declaradas inidôneas pelo Tribunal de Contas da União, site para consulta: https://contas.tcu.gov.br/ords/f?p=INABILITADO:INIDONEOS, nos termos do art. 46 da Lei nº 8.443/92;

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

3.2.6. Que estejam em processo de falência, em recuperação judicial ou extrajudicial, concursos de credores ou insolvência, em processo de dissolução ou liquidação;

3.2.6.1. As sociedades que se encontram em recuperação judicial ou extrajudicial deverão apresentar certidão positiva de recuperação judicial, com a respectiva comprovação da homologação judicial do plano de recuperação.

3.2.7. Empresas em dissolução ou em liquidação, e

3.2.8. Sociedades integrantes de um mesmo grupo econômico, assim entendidas como aquelas que possuam diretores, sócios, representantes legais ou responsáveis técnicos em comum e/ou utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesses comuns.

4. DA APRESENTAÇÃO DA PROPOSTA NA PLATAFORMA ELETRÔNICA

4.1. As empresas interessadas, portadores de chave e senha de acesso, deverão registrar propostas iniciais em conformidade com os requisitos definidos neste Chamamento Público, na plataforma eletrônica: https://licitacoes-e2.bb.com.br/aop-inter-estatico/, cuja reunião pública ocorrerá no dia e horário previsto no cronograma.

4.2. As interessadas deverão encaminhar a PROPOSTA ESCRITA ATUALIZADA concomitantemente com a DOCUMENTAÇÃO DE QUALIFICAÇÃO, conforme itens 6 e 7 deste chamamento público, EXCLUSIVAMENTE POR MEIO DO SISTEMA ELETRÔNICO: https://licitacoes-e2.bb.com.br/aop-inter-estatico/, em até 01 (um) dia útil após a solicitação.

4.3. Eventuais desistências e/ou alterações nas propostas iniciais registradas na plataforma deverão ser realizadas exclusivamente pelos participantes, antes da data e horário de abertura das propostas.

4.4. Será observado o horário de Brasília/DF para todas as referências de tempo contidas neste Chamamento Público.

4.5. A participação neste Processo de Seleção pressupõe o pleno conhecimento e atendimento às regras e exigências de qualificação previstas neste Chamamento Público, e na plataforma do Banco do Brasil, sendo responsável por todas as transações efetuadas.

4.6. Caberá a empresa participante acompanhar alterações de datas/horários, esclarecimentos, erratas e outras comunicações, bem como as operações no sistema eletrônico durante a reunião pública, inclusive das decisões da Comissão de Contratação, sendo responsável exclusivo pelo ônus decorrentes da perda de negócios diante da inobservância de quaisquer mensagens constantes da plataforma e ainda por eventuais perdas de conexão.

4.7. A disputa será conduzida pelo membro da Comissão de Contratação, denominado Condutor do Processo de seleção, que será responsável pelo seu processamento.

4.8. Os interessados em acompanhar a disputa poderão fazê-lo acessando na Internet o endereço eletrônico https://licitacoes-e2.bb.com.br/aop-inter-estatico/, onde se encontra o link do Processo Seletivo.

4.9. Ao cadastrar a proposta no *site* na plataforma eletrônica https://licitacoes-e2.bb.com.br/aop-inter-estatico/, as informações inseridas no campo denominado "Descrição/Observação (Opcional)" tem caráter de preenchimento facultativo e não poderão identificar a empresa participante, visando preservar o sigilo das propostas.

4.10. Para elaboração da proposta a participante deverá considerar que:

4.10.1. O preço total para o lote ofertado deve considerar os impostos diretos e indiretos, taxas, contribuições, fretes, seguros e quaisquer outras incidências fiscais e/ou tributárias e demais custos e despesas incidentes na prestação do serviço;

4.10.2. No caso de lotes com mais de um item, o valor total a ser lançado na plataforma eletrônica, https://licitacoes-e2.bb.com.br/aop-inter-estatico/, é a soma dos valores totais (quantidade x preço unitário) de cada item que compõe o lote;

4.10.3. Não há obrigatoriedade de apresentar ofertas para todos os lotes, entretanto, devem ser cotados todos os itens do mesmo lote;

4.10.4. Os preços cotados e os valores faturados, em moeda corrente nacional, deverão ser fixos e irreajustáveis, não sofrendo qualquer atualização monetária até o seu efetivo pagamento;

4.10.5. Validade mínima da proposta é de 90 (noventa) dias, contados da data da reunião pública;

4.10.6. A base dos preços será a data da reunião pública.

4.10.7. Os serviços ofertados devem corresponder às exigências constantes do Memorial Descritivo, sob pena de desclassificação.

4.10.8. O pagamento será realizado no prazo definido no item 12 – DO PAGAMENTO, não sendo aceita proposta com pagamento antecipado.

4.10.9. Pela elaboração da proposta a empresa participante não terá direito a auferir qualquer vantagem, remuneração ou indenização.

4.11. A proposta final e documentos de qualificação deverão ser anexados pela empresa arrematante, após a disputa, na plataforma https://licitacoes-e2.bb.com.br/aop-inter-estatico/, no prazo de até 01 (um) dia útil após a solicitação do Condutor.

4.12. Do Credenciamento na plataforma https://licitacoes-e2.bb.com.br/aop-inter-estatico/

4.12.1. Para acesso ao sistema eletrônico, os interessados deverão dispor de chave de identificação e senha pessoal, ambas intransferíveis, obtidas junto ao provedor do sistema eletrônico (Banco do Brasil S/A).

4.12.2. As pessoas jurídicas ou empresas individuais deverão credenciar representantes, mediante a apresentação a referida instituição bancária (agência de livre escolha do interessado) de procuração por instrumento público ou particular, com firma reconhecida, atribuindo poderes para formular lances de preços e praticar todos os demais atos e operações no sistema.

4.12.3. Em se tratando de sócio, proprietário ou dirigente da empresa interessada, deverá ser apresentada ao Banco do Brasil S/A cópia do respectivo Estatuto ou Contrato Social e alterações, no qual estejam expressos os poderes para exercer direitos e assumir obrigações.

4.12.4. A chave de identificação e senha terão validade determinada pelo Banco do Brasil S/A, sendo de exclusiva responsabilidade do usuário o sigilo, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao SENAI-SP a responsabilidade por eventuais danos decorrente do uso indevido, ainda que por terceiros.

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

5. DA FASE DE DISPUTA

5.1. A partir do horário previsto no cronograma será iniciada a reunião pública da disputa aberta de preços, cujos preços iniciais serão divulgados.

5.2. O Condutor realizará a disputa, podendo desclassificar as propostas que:

a) Não estiverem em consonância com o exigido neste Chamamento Público, e

b) Apresentem preços irrisórios ou incompatíveis com os preços de mercado, ainda que não se tenha estabelecido limite mínimo.

5.2.1. Tal decisão e outras pertinentes serão registradas na plataforma para acompanhamento das participantes.

5.2.2. A validade do processo de seleção não ficará comprometida, se inviabilizada a fase de lances, em razão da apresentação e/ou classificação de apenas uma empresa, desde que justificada pela Comissão de Contratação, inclusive quanto ao preço.

5.3. Aberta a etapa competitiva, os participantes deverão estar conectados ao sistema para participar da reunião de lances.

5.4. As empresas participantes poderão ofertar lances sem restrição de quantidade ou de qualquer ordem classificatória ou cronológica específica, mas sempre inferior ao seu último lance.

5.5. Todos os lances serão registrados pela plataforma, que indicará sempre o lance de menor valor para acompanhamento em tempo real pelas participantes, mantendo em sigilo os autores dos lances durante a reunião de disputa.

5.6. Será adotado para o envio de lances o modo de disputa “Aberto”, em que os participantes apresentarão lances públicos e sucessivos, com prorrogações.

5.7. Os lances serão ofertados pelo valor global por lote.

5.8. Durante a disputa, as participantes deverão observar o valor estipulado para redução mínima entre os lances subsequentes, em relação ao seu lance anterior e em relação ao melhor lance registrado, para cada lote, conforme abaixo:

LOTE	REDUÇÃO MÍNIMA ENTRE OS LANCES SUBSEQUENTES DA MESMA PARTICIPANTE	REDUÇÃO MÍNIMA EM RELAÇÃO AO MELHOR LANCE
01	R$ 5.000,00	R$ 5.000,00

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

5.8.1.1. A prorrogação automática da etapa de lances será de 02 (dois) minutos e ocorrerá sucessivamente, sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.8.1.2. Não havendo lances na forma estabelecida no item anterior, a sessão pública encerrar-se-á automaticamente.

5.8.2. A exclusão de lance somente será possível pelo fornecedor durante a fase de lances, dentro do prazo de 15 (quinze) segundos, conforme possibilita o sistema eletrônico, ou seja, antes do encerramento do lote.

5.8.3. No caso de desconexão do Condutor, durante a etapa de lances, se o sistema permanecer acessível aos participantes, os lances continuarão sendo recebidos sem prejuízo dos atos realizados.

5.8.4. Encerrada a disputa, o sistema informará a proposta de menor preço. O condutor do processo solicitará, no campo "*chat de mensagem*", o envio da PROPOSTA ESCRITA ATUALIZADA E DOCUMENTOS DE QUALIFICAÇÃO correspondentes, para acesso público e avaliação do condutor, sendo necessariamente, inseridos pelo arrematante em até 01 (um) dia útil após solicitação na plataforma https://licitacoes-e2.bb.com.br/aop-inter-estatico/.

5.8.4.1. O Condutor poderá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao participante arrematante do lote, com vistas a redução do preço, decidindo sobre sua aceitação.

5.8.4.2. Caso o preço resultado desta negociação, ainda esteja incompatível com o mercado, o Condutor poderá convocar o participante subsequente para que tenha a mesma oportunidade e assim, sucessivamente.

5.8.5. A ausência da documentação, após o prazo de solicitação, ocasionará na desclassificação do participante e a convocação do próximo colocado em preço.

6. DA PROPOSTA ESCRITA FINAL

6.1. A proposta final e demais anexos deverão ser anexados pela arrematante, no prazo estabelecido no subitem 4.11, do item 4 deste Chamamento deste instrumento, o qual poderá ser prorrogado por igual período a critério da Comissão de Contratação, devendo neste caso, ser utilizado o mesmo critério para as demais participantes.

6.2. **Proposta Comercial**

6.2.1.1. Proposta de preços, com identificação da participante e do lote arrematado, conforme Modelo de Proposta, Anexo C.

6.2.1.2. O preço da proposta comercial escrita deverá ser o mesmo ofertado por lance durante a disputa eletrônica, salvo se houver tratativas realizadas com o Condutor, para obtenção de preço menor.

6.2.1.3. A proposta e a documentação de qualificação da arrematante serão analisadas pela Comissão de Contratação, que poderá se valer de assessoramento da área técnica e jurídica do SENAI-SP, quando for o caso, podendo ser realizadas diligências para confirmação das informações contidas nos documentos apresentados e o atendimento as especificações exigidas, por meio de esclarecimentos ou informações complementares.

6.2.1.4. A inobservância da exigência, no prazo de 2 (dois) dias úteis, resultará na desclassificação da proposta para o lote correspondente.

7. DA DOCUMENTAÇÃO DE QUALIFICAÇÃO

7.1. Os documentos de qualificação, citados neste subitem, bem como a documentação citada no subitem 6, devem ser anexados, na plataforma eletrônica: https://licitacoes-e2.bb.com.br/aop-inter-estatico/, em até 01 (um) dia útil, após a solicitação, a saber:

7.1.1. Modelo de declaração sobre emprego de menor e outras informações, Anexo A, concordando com os termos do Chamamento Público, credenciando o representante legal perante o SENAI-SP para todos os assuntos pertinentes ao presente Processo de Seleção, entre outros.

7.1.2. Prova de inscrição e de situação cadastral ativa no Cadastro Nacional de Pessoas Jurídicas (CNPJ).

7.1.3. Prova de inscrição no Cadastro de Contribuinte Estadual, relativa ao domicílio ou sede da participante, pertinente ao seu ramo de atividade e compatível com o objeto a ser contratado.

7.1.4. Prova de inscrição no Cadastro de Contribuinte Municipal, relativa ao domicílio ou sede da participante, pertinente ao seu ramo de atividade e compatível com o objeto a ser contratado.

7.1.5. Prova de regularidade com a Fazenda Nacional (certidão negativa de débitos relativos aos tributos federais e à Dívida Ativa da União), que abrangem as contribuições previdenciárias.

7.1.6. Prova de regularidade para com a Fazenda Estadual, do domicílio ou sede do participante, consubstanciada na Certidão expedida pela Secretaria de Estado dos Negócios da Fazenda e/ou Procuradoria Geral do Estado.

7.1.7. Prova de regularidade para com a Fazenda Municipal, referente a tributos mobiliários do domicílio ou sede do participante.

7.1.8. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço - FGTS, do domicílio ou sede da participante.

Obs.: Serão aceitas certidões positivas com efeito de negativa.

7.2. Os documentos de qualificação, bem como quaisquer outros solicitados, deverão estar válidos na data da disputa.

8. DA ANÁLISE E JULGAMENTO DAS PROPOSTAS E DA DOCUMENTAÇÃO DE QUALIFICAÇÃO

8.1. A Comissão de Contratação poderá se valer de assessoramento técnico para análise das propostas e documentação de qualificação apresentadas pelas participantes, os quais emitirão pareceres que subsidiarão as tomadas de decisões.

8.2. A critério da Comissão de Contratação, eventuais falhas ou omissões formais poderão ser relevados, desde que não resultem em prejuízo para o entendimento das propostas.

8.3. Não serão aceitos “protocolos de entrega” ou “solicitação de documento” em substituição aos documentos requeridos no presente Chamamento Público.

8.4. Durante o Processo de Seleção, é facultado a Comissão de Contratação ou aos técnicos por ela designados realizar diligências para esclarecimentos e informações complementares, bem como conceder prazo para que os participantes adequem suas propostas e documentos de qualificação, visando sanar eventuais omissões ou inadequações.

8.4.1. A critério da Comissão de Contratação poderão ser aceitos documentos que, embora não entregues quando da convocação, estavam vigentes e/ou válidos na data da disputa.

8.5. Todos os cálculos serão efetuados com duas casas decimais, desprezando-se sempre a fração remanescente.

8.6. A análise das propostas, observará a ordem da classificação, resultante da disputa de preços, restringindo-se, a princípio, à proposta apresentada pela arrematante, desde que atenda plenamente as exigências deste Chamamento Público, caso contrário, será avaliada a proposta subsequente e assim sucessivamente, até a obtenção de proposta válida.

8.6.1. Visando à celeridade do processo, a critério da Comissão de Contratação, poderá ser solicitada proposta final das próximas colocadas, para análise simultânea e concomitantemente.

8.7. O Condutor poderá negociar com as participantes, observando a ordem de classificação das propostas, visando a redução dos preços e adequação ao mercado.

8.8. Serão desclassificadas as participantes:

8.8.1. Nas situações previstas no item 3.2;

8.8.2. Cujas propostas não atendam às exigências constantes do Memorial Descritivo;

8.8.3. Na apresentação de declarações emitidas por empresas que mantenham vínculo societário ou qualquer outra forma de relação direta ou indireta com a participante, tais como participação comercial, técnica, econômica ou financeira;

8.8.4. Que deixarem de apresentar os documentos solicitados nos itens 6. DA PROPOSTA ESCRITA FINAL E 7. DA DOCUMENTAÇÃO DE QUALIFICAÇÃO, exceto do Anexo A – visto que a entrega da proposta implica na aceitação formal das condições estabelecidas neste Chamamento Público.

8.9. O não atendimento aos requisitos e dos prazos estipulados neste Chamamento Público, a participante será desclassificada, cabendo ao Condutor registrar e disponibilizar a decisão no sistema eletrônico para acompanhamento em tempo real pelas participantes.

8.10. Caso haja desistência da proposta, a critério exclusivo do SENAI-SP, a participante poderá ser penalizada com a suspensão do direito de contratar com o SESI-SP e SENAI-SP, por um período de até 05 (cinco) anos.

8.11. Constatado o atendimento dos requisitos previstos neste Chamamento Público, a participante será classificada e considerada apta para contratação.

8.12. Caso haja empate entre duas ou mais propostas, prevalecerá a primeiramente registrada, desde que tenha atendido a todos os requisitos exigidos neste Chamamento Público.

8.13. Na hipótese de desclassificação de todos os participantes, o SENAI-SP poderá fixar novo prazo para apresentação de outras propostas ou de novos documentos, escoimados das causas que implicaram na desclassificação.

8.14. O resultado dessas análises será submetido à Comissão de Contratação, sendo as decisões lavradas em atas e disponibilizadas às participantes na plataforma https://licitacoes-e2.bb.com.br/aop-inter-estatico/, abrindo-se o prazo para apresentação de pedido de reconsideração.

9. DOS PEDIDOS ESCLARECIMENTOS E DE RECONSIDERAÇÃO

9.1. As eventuais dúvidas deverão ser encaminhadas, até a data prevista no cronograma anexo, através do e-mail: contratacaodebens03@sesisenaisp.org.br c/c paulo.neto@sesisenaisp.org.br, à Gerência de Compras – GC, mencionando o número do Processo de Seleção e o objeto da contratação.

9.1.1. As respostas, eventuais esclarecimentos e/ou alterações serão disponibilizadas às interessadas no endereço eletrônico: https://transparencia.sp.senai.br/licitacoes-editais, até a data prevista no cronograma, sem, porém, identificar o formulador da consulta, as quais passarão a valer como normas.

9.2. Das decisões proferidas quanto a qualificação das participantes e de suas propostas, caberá pedido de reconsideração à Comissão de Contratação, no prazo de 02 (dois) dias úteis após a divulgação do resultado de cada participante, na plataforma do https://licitacoes-e2.bb.com.br/aop-inter-estatico/, a ser encaminhado através do e-mail: contratacaodebens03@sesisenaisp.org.br c/c paulo.neto@sesisenaisp.org.br.

9.2.1. As participantes, cuja situação no processo possa ser afetada, poderão se manifestar sobre o pedido de reconsideração, no prazo de 02 (dois) dias úteis, a contar da divulgação do resultado de cada participante, na plataforma do https://licitacoes-e2.bb.com.br/aop-inter-estatico/.

9.2.2. Havendo pedido de reconsideração, o prazo de validade das propostas será suspenso, reiniciando-se a contagem a partir da divulgação do resultado.

9.3. Da decisão da Comissão de Contratação relativa ao pedido de reconsideração não caberá novo pedido de reconsideração.

9.4. Definido o resultado pela Comissão de Contratação e não havendo pedidos de reconsideração ou sendo estes devidamente analisados e respondidos, o Processo de Seleção seguirá para conclusão.

10. DA CONTRATAÇÃO

10.1. As condições estabelecidas neste Chamamento Público, no que se aplicar, farão parte do contrato e/ou pedido de compra correspondente, independentemente de transcrição em seu texto.

10.2. Após aprovação do Processo de Seleção, a participante selecionada será notificada para assinatura do contrato no prazo de 02 (dois) dias úteis, conforme as respectivas minutas, **Anexo D**.

10.2.1. A documentação de qualificação apresentada na plataforma eletrônica será utilizada para a realização do Cadastro da participante selecionada. Entretanto, quando da assinatura do contrato, poderá haver necessidade de atualização da documentação, em parte ou no todo, que deverá ser providenciada pela empresa a ser contratada, no prazo de até 02 (dois) dias úteis.

10.2.1.1. O prazo acima estabelecido poderá ser prorrogado, a critério exclusivo da Comissão de Contratação.

10.3. Caso a participante selecionada não assine o contrato e/ou não apresente a documentação regular, no prazo de até 02 (dois) dias úteis, a critério exclusivo do SENAI-SP, a mesma poderá ser penalizada com a suspensão do direito de contratar com o SESI e SENAI, por um período de até 05 (cinco) anos e/ou aplicadas as penalidades previstas no item 13 – DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES. Nesse caso, o SENAI-SP poderá convocar as participantes remanescentes para fazê-lo, observada a ordem de classificação, ou realizar novo Processo de Seleção.

10.4. Antes da assinatura do contrato, o SENAI-SP poderá desclassificar a participante selecionada, caso tenha conhecimento de qualquer fato anterior ou posterior ao julgamento deste Processo de Seleção que venha desaboná-la técnica, financeira ou administrativamente, não lhe cabendo direito a qualquer reclamação, indenização ou ressarcimento.

10.5. O futuro contrato vigorará pelo prazo de 12 (doze) meses, podendo ser renovado através da elaboração do competente Termo Aditivo, até o limite máximo de 36 meses, respeitadas as demais previsões contidas nos artigos 34 e 38 do RCA.

10.6. A critério das partes, após o 12º mês de vigência contratual, havendo prorrogação do contrato, poderá ser aplicado o reajustamento de preço anual com base no índice IPCA/IBGE acumulado nos últimos 12 meses, relativo ao mês anterior (11º mês), ou, mediante concordância entre as partes, referente ao segundo mês anterior ao 12º (10º mês), ou ainda, por outro índice que venha a substituí-los, caso haja a extinção de um deles.

10.7. Qualquer uma das partes poderá rescindir o contrato antecipadamente, desde que comunique sua intenção com no mínimo 60 (sessenta) dias de antecedência.

11. DAS OBRIGAÇÕES DA CONTRATADA

11.1. Obrigações da contratada:

11.1.1. Executar os serviços, objeto deste Chamamento Público, de acordo com as exigências definidas no Memorial Descritivo, Minuta de Contrato e demais anexos.

11.1.2. Responsabilizar-se, em caráter exclusivo, pela execução dos serviços por seus empregados, prepostos, parceiros e terceiros.

11.1.3. Executar os serviços nos prazos estabelecidos no Memorial Descritivo, Minuta de Contrato e demais anexos.

11.1.4. Arcar com eventuais custos de transporte, estadia, alimentação entre outros, necessários à execução dos serviços.

11.1.5. Considerar a vistoria e aceitação dos serviços por técnicos do SENAI-SP, se for o caso.

11.1.6. Notificar por escrito ao SENAI-SP, ao gestor do Contrato, caso ocorra qualquer fato que impossibilite o cumprimento das condições e prazos estabelecidos no contrato.

11.1.7. Responsabilizar-se por todos e quaisquer danos e/ou prejuízos que venham a causar ao SENAI-SP.

11.1.8. Solucionar eventuais falhas sem ônus ao SENAI.

11.1.9. Manter, durante o tempo de vigência do contrato, os documentos de regularidade fiscal e regularidade técnica devidamente atualizados.

11.2. Os serviços inerentes à esta contratação serão conduzidos sob a fiscalização Gerência de Infraestrutura e Suprimentos, que indicará funcionário que exercerá a função de Gestor do Contrato, responsável por acompanhar a execução, as etapas e prazos determinados, conferir os documentos e relatórios pertinentes, atestar a realização dos serviços e liberar os pagamentos correspondentes.

11.3. Respeitadas todas as previsões descritas neste chamamento, no memorial descritivo e na minuta de contrato, a Contratada é a única e exclusiva responsável por todos os encargos trabalhistas, inclusive decorrentes de acordos, dissídios e convenções coletivas, previdenciários, fiscais e comerciais, oriundos da execução do contrato, podendo o SENAI-SP a qualquer tempo, exigirem a comprovação do cumprimento de tais encargos, como condição do pagamento do valor ajustado no contrato.

12. DO PAGAMENTO

12.1. O(s) pagamento(s) será(ão) efetuado(s) no mês subsequente ao da prestação de serviços e ocorrerão 10 (dez) dias após o recebimento da nota fiscal/fatura, fora a dezena, de modo que ocorram somente nos dias 10, 20 ou 30 de cada mês.

12.1.1. Quando recaírem em finais de semana e feriados, o pagamento será realizado no primeiro dia útil subsequente; no mês de fevereiro, os pagamentos serão realizados nos dias 10, 20 e 28 (ou 29, se o ano for bissexto).

12.2. Os serviços de manutenção dos equipamentos serão validados por técnicos do SENAI-SP. A Contratada deverá emitir notas fiscais distintas para as respectivas unidades do SENAI-SP, onde ocorreram os serviços: Escola Senai de Lençóis Paulista, Rua Aristeu Rodrigues Sampaio, 271, Bairro Jardim das Nações, Lençóis Paulista/SP, CEP 18685-730 e Escola Senai de São Bernardo do Campo, Rua Vitória Maria Médice Ramos, 330 - Assunção - São Bernardo do Campo-São Paulo, CEP: 09861-790.

12.3. Os pagamentos serão efetuados diretamente pela Gerência Sênior Contábil e Financeira do SENAI-SP, situada na Avenida Paulista, nº 1313, 2º andar, Bairro Bela Vista, em São Paulo – SP.

12.4. Para contagem do prazo de pagamento, considerar-se-á o dia da entrega da Nota Fiscal / Fatura, devidamente validada pelo Gestor do Contrato.

12.5. O SENAI-SP, em conformidade com a legislação vigente, reterá do valor bruto da Nota Fiscal / Fatura, as alíquotas referentes aos impostos/taxas: IR, INSS, ISS, CSLL, COFINS, PIS/PASEP, entre outros, os quais deverão estar devidamente destacados no documento fiscal.

12.6. Os pagamentos serão efetuados através de depósito bancário, devendo ser encaminhadas, obrigatoriamente, as duplicatas e/ou recibos devidamente quitados. Não deverão ser emitidos boletos bancários, bem como, não é permitido negociar os títulos.

13. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

13.1. **À Participante:**

13.1.1. O não atendimento das exigências previstas neste Chamamento Público, dos compromissos assumidos, bem como, se for constatado inveracidade de quaisquer informações e/ou documentos fornecidos, poderá implicar, à participante, a penalidade de desclassificação da proposta e consequente exclusão do Processo de Seleção.

13.1.2. A recusa injustificada ou não aceita pelo SENAI-SP em assinar o contrato e/ou os pedidos de compra, dentro do prazo fixado, caracterizará o descumprimento total das obrigações assumidas e poderá acarretar às seguintes penalidades:

a) perda do direito à contratação, e

b) suspensão do direito de contratar com o SESI e SENAI pelo prazo de até 05 (cinco) anos.

13.2. **À Contratada:**

13.2.1. O atraso ou o descumprimento de quaisquer obrigações, acarretará a aplicação de advertência e/ou multa no percentual de 2% (dois por cento) do valor total do contrato.

13.2.2. O inadimplemento total ou parcial das obrigações assumidas pela contratada, dará ao SENAI-SP o direito de rescindir unilateralmente o contrato e/ou pedidos de compra, sem prejuízo da aplicação de outras penalidades previstas neste Chamamento Público, inclusive a de suspensão do direito de contratar com o SESI e SENAI por prazo de até 05 (cinco) anos.

13.2.3. A parte que der motivo à rescisão por atrasos, descumprimento das cláusulas e condições constantes do contrato, incorrerá no pagamento, à parte inocente, da multa equivalente a 10% (dez por cento) do valor total do contrato ressalvado o direito ao credor de exigir indenização por prejuízo excedente, nos termos do parágrafo único do art. 416 do Código Civil.

13.3. As penalidades previstas são independentes, não excludentes e poderão ser aplicadas cumulativamente

13.4. Os valores relativos as multas aplicadas, bem como, outros valores que forem devidos serão deduzidos dos créditos que a contratada possuir com o SENAI-SP ou cobrados administrativa ou judicialmente.

14. CASOS OMISSOS

14.1. Qualquer caso omisso no decurso deste Chamamento Público será dirimido pela Comissão de Contratação e produzirá seus efeitos.

São Paulo, 03 de dezembro de 2025.

Gerência de Compras – GC
Serviço Nacional de Aprendizagem Industrial – SENAI
Departamento Regional de São Paulo

CRONOGRAMA

PROCESSO DE SELEÇÃO COM DISPUTA ABERTA N.º 895/2025

CONTRATAÇÃO DE PLATAFORMA DE SIMULAÇÃO DE ATAQUE E DEFESA CIBERNÉTICA HIPER-REALISTA

Eventos	Datas
Publicação	**03/12/2025**
Retirada do Chamamento Público	A partir de 03/12/2025 *site*: https://licitacoes-e2.bb.com.br/aop-inter-estatico/
Pedidos de Esclarecimentos	**De 03/12/2025 até 08/12/2025** *e-mail*: contratacaodebens03@sesisenaisp.org.br paulo.neto@sesisenaisp.org.br
Início da reunião pública de disputa de preços	**11/12/2025** às **09h30min**

ANEXO A

MODELO DE DECLARAÇÃO SOBRE EMPREGO DE MENOR E OUTRAS INFORMAÇÕES
(*em papel timbrado da participante)*

Ao
Serviço Nacional de Aprendizagem Industrial (SENAI)
Gerência de Compras - GC

PROCESSO DE SELEÇÃO N. º 895/2025

DADOS DA EMPRESA	
Razão Social:	
Endereço completo:	
Telefone:	*E-mail*:
CNPJ:	

SÓCIOS E ADMINISTRADORES	
Nome:	Qualificação:
Nome:	Qualificação:

DADOS DO REPRESENTANTE LEGAL	
Nome:	Cargo:
CPF:	RG:
Telefone:	*E-mail*:

DADOS DO CONTADOR OU DA EMPRESA DE CONTABILIDADE		
Nome do Contador:		CRC:
Razão Social:	CNPJ:	CRC do responsável:

DADOS BANCÁRIOS DA EMPRESA PARA PAGAMENTO (se houver possibilidade de pagamentos em mais de uma conta, lista todas as possíveis)		
Banco:	Agência:	Conta Corrente:

Declaramos sob as penalidades da Lei, para fins do Processo de Seleção acima referido que:

a) concorda com as condições e regras deste Chamamento Público;
b) na composição societária não existe participação de dirigentes ou empregados do SENAI-SP;
c) na composição societária não existe participação de dirigentes ou sócios de qualquer outra participante do referido processo de seleção;
d) à elaboração da proposta é de nossa responsabilidade,
e) não empregamos menores de 18 anos em trabalho noturno, perigoso ou insalubre e nem menores de 16 anos, em qualquer trabalho, salvo na condição de aprendiz a partir de 14 anos, e
f) que concordamos com a Política de Proteção de Dados Pessoais e Privacidade do SENAI-SP, disponibilizada no link: https://privacidade.sp.senai.br.

(Local e Data)

_____

(Nome completo e assinatura do representante legal)

ANEXO B

MEMORIAL DESCRITIVO

1. Objeto

1.1. Contratação de solução com ambiente hiper-realista para a simulação de ataques cibernéticos em sistemas de Tecnologia da Informação (TI), por meio do fornecimento de licenças no modelo SaaS (Software as a service).

1.2. A solução hiper-realista para a simulação de ataques cibernéticos, doravante denominada Solução de Segurança Cibernética, é um ambiente virtual que permite a simulação ambientes de ataque e defesa cibernéticos em diversos cenários e vírus emulados.

1.3. A Solução de Segurança Cibernética deve contemplar:

1.3.1. Fornecimento de 10 (dez) licenças no modelo SaaS por, pelo menos, 12 (doze) meses de permissão de uso.
1.3.2. Pacote mínimo de 50 (cinquenta) cenários nos níveis básico, intermediário e avançado;
1.3.3. Backup e Restore;
1.3.4. Sustentação;
1.3.5. Suporte ao Usuário.

2. Justificativa

2.1. De acordo com a Kaspersky, cibersegurança é a prática de proteger sistemas, dispositivos e dados contra-ataques maliciosos. Também conhecida como segurança da tecnologia da informação, abrange desde a proteção de redes até a conscientização dos usuários. Protocolos de criptografia são utilizados para codificar e-mails, arquivos e informações, protegendo dados durante a transmissão e evitando perdas ou roubos.

2.2. O portal Afrika destaca que governos, empresas e instituições processam grandes volumes de informações confidenciais em redes globais. Com o aumento dos ataques cibernéticos, proteger dados e garantir a segurança nacional tornou-se essencial.

2.3. Na Quarta Revolução Industrial, tecnologias como Sistemas Ciberfísicos (CPS) e Internet das Coisas (IoT), geram enormes volumes de dados que, sem proteção adequada, podem comprometer a segurança de pessoas e operações. Investir na formação de profissionais em cibersegurança é crucial para atender às demandas da Indústria 4.0.

2.4. No entanto, a situação da cibersegurança no Brasil é preocupante. Segundo o portal Convergência Digital, um levantamento do Instituto Ponemon revela que 58% das empresas brasileiras não oferecem treinamento em cibersegurança aos funcionários, e apenas 10% planejam fazê-lo nos próximos 12 meses. Além disso, 75% dos profissionais apontam como maiores riscos o roubo de propriedade intelectual, violação de dados de clientes e prejuízos causados por interrupções nos sistemas.

2.5. Esses dados reforçam a necessidade urgente de corrigir a lacuna entre as equipes de segurança e os executivos, além de investir na capacitação de equipes para enfrentar as ameaças cibernéticas em um mundo cada vez mais conectado.

2.6. Considerando este cenário, a Solução de Segurança Cibernética será integrada a diversas unidades curriculares dos cursos superiores, abrangendo disciplinas como Coleta de Informação, Pentesting em Redes, Análise Forense Digital e Hardening. Ela também será aplicada em atividades práticas nos cursos técnicos de Redes de Computadores e Desenvolvimento de Sistemas, bem como nos cursos FIC de alto valor agregado. As simulações, incluindo exercícios como Capture the Flag (CTFs), proporcionarão uma formação diferenciada aos alunos.

2.7. Os ganhos institucionais são significativos, uma vez que a plataforma promoverá um aprendizado ativo, alinhado às mais recentes tendências e ameaças cibernéticas, fortalecendo a oferta de cursos técnicos, superiores e livres. Além disso, contribuirá para a elevação da empregabilidade dos egressos, capacitando-os com habilidades avançadas e diferenciadas para atuar no mercado de trabalho.

3. Características dos Serviços

3.1. Escopo:

3.1.1. O presente processo trata do fornecimento de 10 (dez) licenças de uso SaaS (Software as a Service) simultâneo, em um ambiente simulado de ataque e defesa cibernética, com cenários básicos, intermediários e avançados.

3.2. Características Técnicas Gerais

3.2.1. A especificação técnica da Solução de Segurança Cibernética será detalhada no documento anexo Termo de Referência. A seguir um breve resumo dos requisitos:

3.2.2. Tecnologias: Permite a criação de ambientes simulados realistas que replicam redes de computadores, servidores, dispositivos e serviços;

3.2.2.1. Tecnologia de virtualização para criar e gerenciar máquinas virtuais;

3.2.2.2. Integração de redes físicas e virtuais para simulação de ambiente híbrido;

3.2.2.3. Geração de tráfego simulado realista.

3.2.3. Perfis de Usuários:

3.2.3.1. Suporte a diferentes perfis de usuários;

3.2.3.2. Instrutor: Aplica configurações em simulações, monitora o progresso dos participantes, avalia o desempenho e gera relatórios. Tem acesso a ferramentas de supervisão em tempo real e pode intervir nas simulações conforme necessário;

3.2.3.3. Participante: Participa dos exercícios práticos em cenários simulados, interagindo com os ambientes criados e realizando tarefas designadas. Pode acessar feedback e resultados de desempenho para aprimorar suas habilidades.

3.2.4. Objetos:

3.2.4.1. Disponibilizar objetos virtualizados e permitir a integração de objetos especiais, como emuladores e dispositivos físicos externos:

3.2.4.1.1. Objetos Virtualizados: Incluem sistemas operacionais (Windows, Linux), aplicativos (servidores web, bancos de dados), ferramentas de segurança (IDS/IPS, antivírus) e dispositivos de rede (switches, roteadores);

3.2.4.1.2. Objetos Especiais: Emuladores que replicam o comportamento de dispositivos reais, como sensores IoT, appliances de segurança e equipamentos industriais;

3.2.4.1.3. Integração Física: Capacidade de conectar dispositivos físicos ao ambiente simulado, permitindo interações reais em um contexto virtual;

3.2.4.1.4. Gerenciamento total dos endereços IP, permitindo criar endereços reais em ambiente apartado.

3.2.5. Automação de Eventos

3.2.5.1. Permitir execução de ações automatizadas e manuais durante os exercícios.

3.2.5.2. Eventos Automatizados: Scripts que executam ações predefinidas, como ataques DDoS, exploração de vulnerabilidades, mudanças na configuração de rede e respostas automáticas a incidentes;

3.2.5.3. Eventos Manuais: Ações que podem ser disparadas pelo instrutor durante a simulação para ajustar o cenário ou introduzir novos desafios;

3.2.5.4. Monitoramento em Tempo Real: Ferramentas para monitorar a execução de eventos e o comportamento dos participantes, permitindo ajustes imediatos;

3.2.5.5. Adição de Marcos e Snapshots: Criação de pontos de verificação para salvar o estado do cenário.

4. Licença, Garantias e Prazos

4.1. As licenças poderão ser utilizadas durante todo o período de referência, por quantas vezes o entender necessário e por quantos usuários for indicado, até o limite contratado, sem que seja caracterizado o uso de novas licenças.

4.2. Os serviços executados no escopo da presente contratação terão garantia irrestrita durante a vigência integral do contrato, inclusive para os períodos de prorrogações.

4.3. Poderá solicitar, dentro do período de garantia, sem qualquer ônus adicional, a correção ou nova execução de serviços, produtos ou documentos entregues que apresentem problemas ou necessidade de correções.

4.4. Deverá assegurar garantia durante 12 (doze) meses para todos os itens do software fornecido, inclusive para os períodos de eventuais prorrogações do contrato.

4.5. A garantia inclui as atualizações de softwares fornecidos e portabilidade de softwares, ambos dentro dos prazos vigentes do contrato, sem ônus financeiro adicional.

4.6. A Contratada deverá assegurar o fornecimento das licenças para acesso à plataforma durante 12 (doze) meses, a contar a partir da liberação do acesso, para todos as funcionalidades contratadas, mencionadas no item 3.2.1. Este contrato poderá se estender em até 36 (trinta e seis) meses, com pagamentos anuais, caso ambas as partes decidam por renovar a contratação, podendo sofrer reajuste de valor após o 12º mês, conforme item 10.5 deste Chamamento.

4.7. O prazo para liberação de acesso à plataforma é de até 05 (cinco) dias úteis após o envio do pedido de compra. Eventuais prazos adicionais de implantação serão integrados à vigência contratual e de acesso à referida plataforma.

5. Obrigações Da Contratada

5.1. Manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas no processo licitatório, necessárias para que todos os níveis de serviços acordados, sejam cumpridos com utilização eficiente dos recursos disponíveis.

5.2. Responsabilizar-se pelo cumprimento das exigências legais no que respeita às jornadas das equipes de trabalho, em seus diversos horários.

5.3. Assumir a responsabilidade por todos os encargos fiscais, previdenciários e obrigações previstas na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria.

5.4. Guardar sigilo dos dados a que tiver acesso ou que vierem a ser compartilhados, bem como sobre os produtos de propriedade do SENAI-SP, além daqueles processados e gerados no ambiente físico da Contratada, reconhecendo serem estes de propriedade exclusiva do SENAI-SP, os quais não podem ser cedidos, copiados, reproduzidos, publicados, divulgados de nenhuma forma, nem colocados à disposição direta ou indiretamente, locados ou vendidos a terceiros.

5.5. Responsabilizar-se pelos danos financeiros ou de imagem causados diretamente ao SENAI-SP ou a terceiros, até o limite do contrato, decorrentes de sua culpa ou dolo quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento pela Gerência Sênior de Tecnologia da Informação do SENAI-SP.

5.6. Apresentar, quando solicitado, a licença de uso ou certificação de posse de todos os softwares de sua propriedade que serão empregados na prestação dos serviços, não cabendo ao

SENAI-SP quaisquer ônus decorrentes do uso indevido de softwares pela equipe técnica da Contratada.

5.7. Responsabilizar-se pelo cumprimento da legislação competente por qualquer item de reparo no ambiente, não cabendo ao SENAI-SP quaisquer ônus decorrentes.

5.8. Cumprir demais obrigações descritas na minuta de chamamento público e na minuta de contrato.

6. Obrigações do SENAI-SP

6.1. Fornecer à Contratada, em tempo hábil, as informações necessárias à execução dos serviços, bem como a documentação técnica referente aos padrões adotados, se necessário.

6.2. Informar à Contratada as normas e procedimentos de acesso às instalações da Gerência Sênior de Tecnologia da Informação do SENAI-SP e suas eventuais alterações.

6.3. Designar um funcionário para gerenciar e fiscalizar o contrato.

6.4. Anotar em registro próprio todas as ocorrências relacionadas à execução dos serviços mencionados, determinando o que for necessário à regularização das falhas ou defeitos observados.

7. Do Pagamento

7.1. Os pagamentos serão feitos a partir da validação da unidade requisitante, de acordo com a autorização para faturamento ou documento equivalente emitido pelo SENAI-SP.

7.2. Uma vez aceitos os serviços pelo SENAI-SP, a Contratada deverá emitir as faturas correspondentes, com os pagamentos sendo efetuados em 30 (trinta) dias corridos após a data efetiva da entrega confirmada, fora a dezena, de modo que ocorram somente nos dias 10, 20 ou 30 de cada mês.

7.3. Quando estes recaírem em finais de semana e feriados, o pagamento será realizado no 1º dia útil subsequente.

7.4. Os pagamentos relativos ao mês de fevereiro ocorrerão nos dias 10, 20 e 28 ou 29 (ano bissexto).

7.5. Fica vedada a negociação de duplicatas com terceiros, bem como o desconto ou a promoção de cobrança através da rede bancária.

7.6. Os pagamentos serão efetuados através de depósito bancário. Para tanto, deverão ser encaminhadas, obrigatoriamente, as duplicatas e/ou recibos devidamente quitados.

7.7. Não deverão ser emitidos boletos bancários, bem como, não é permitido negociar os títulos.

8. Vigência Contratual

8.1. O contrato vigorará pelo prazo de 12 (doze) meses, podendo ser renovado por meio da elaboração de Termo Aditivo, até o limite máximo de 36 (trinta e seis) meses, respeitadas as demais previsões contidas no artigo 34 e 38 do RCA do SENAI.

8.2. Fica convencionado que na hipótese de prorrogação do prazo contratual, poderá, a critério das partes, após o 12º (anual) mês de vigência do ajuste, ser aplicado o reajustamento de preço com base na variação da média aritmética simples da variação acumulada nos últimos 12 meses, do IPCA, relativo ao mês anterior do término de vigência do contrato ou, mediante concordância entre as partes, referente ao segundo mês anterior ao vencimento do contrato, ou, ainda, por outro índice que venha a substituí-los, caso haja a extinção de um deles.

-XXX-

Anexo I – Termo de Referência
Anexo II – Requisitos de Segurança da Informação e Privacidade
Anexo III – Checklist – Requisitos de Segurança da Informação / Requisitos de Privacidade e Conformidade LGPD

Detalhamento Técnico da Solução de Segurança Cibernética

1. Acessos Simultâneos

A tabela a seguir detalha os quantitativos estimados para a operação que deverão ser atendidos pela Solução:

Item	Perfil	Descrição	Quantidade Estimada
A	Usuário Final	Usuários consumidores dos conteúdos gerados e/ou disponibilizados na Plataforma	Até 10 usuários, simultâneos.

2. Backup e Restore

2.1.1. A CONTRATADA se responsabilizará pela execução das rotinas de backup e restore, seguindo a política aprovada pelo SENAI-SP.

2.1.2. A CONTRATADA deverá adotar política de backup e restore que permita a restauração integral da infraestrutura necessária ao processamento normal dos sistemas de informação que compõem a Plataforma, bem como recursos de disaster recovery, incluindo todos os elementos de software do ambiente, tais como:

2.1.2.1. Sistemas operacionais, sistemas gerenciadores de banco de dados, internet information system, sistemas de gerenciamento de correio eletrônico, domain control, file server, dlls, registry etc., com suas respectivas configurações.

2.1.2.2. Sistemas de Informação, softwares e aplicações, inclusive rotinas, procedures etc., com suas respectivas configurações.

2.1.2.3. Tabelas, dados, imagens, áudio, vídeo, armazenados internamente nos servidores, em unidades de armazenamento, inclusive os que são utilizados pelo servidor de arquivos, sistemas de correio eletrônico e aplicações em geral.

2.1.3. O backup das bases de dados de aplicações de execução contínua deverá ser realizado sem interrupção dos serviços (backup on-line).

2.1.4. Os servidores para realização da atividade de backup deverão ter alta capacidade, unidades robotizadas e programas específicos para implementação automática dos processos de backup e restore.

2.1.5. Deverá ser utilizada uma rede de alta velocidade, totalmente independente da rede de dados, evitando que o tráfego de backup afete a operação normal dos sistemas.

2.1.6. Antes da execução da aplicação de correções em qualquer servidor do ambiente de produção, bem como instalação de software ou mudança de hardware, deverá ser feito backup full do mesmo, que deverá ser retido por pelo menos 90 (noventa) dias. Eventual necessidade de interrupção dos serviços para realização do backup será computada no tempo de duração da intervenção.

3. Sustentação e Suporte

3.1. Sustentação

3.1.1. Entende-se como sustentação a execução de todos os serviços necessários para operação em regime "24x7x365" (vinte e quatro horas por dia, sete dias por semana, ao longo do ano), manutenções preventivas/corretivas, atualização da aplicação e seus componentes, suporte aos produtos da Plataforma com os seus respectivos componentes e gerenciamento completo dos equipamentos, serviços e softwares relativos ao escopo contratado.

3.1.2. O monitoramento da infraestrutura integrada será em regime integral, proativo, envolvendo todos os ambientes (Sistemas Operacionais, Web/App, Bancos de Dados, Rede, Armazenamento de Dados e Produtos Básicos).

3.1.3. As novas versões da Plataforma, decorrentes dos serviços de sustentação, deverão atender às mesmas exigências previstas neste documento para a versão original.

3.1.4. Quaisquer serviços ou procedimentos realizados deverão ser previamente autorizados pelo SENAI-SP.

3.1.5. **Abertura de chamados de sustentação:**

3.1.5.1. Os chamados representam a solicitação formal de serviços de sustentação à CONTRATADA e devem ser atendidos de acordo com os critérios e parâmetros estabelecidos para execução dos serviços conforme estabelecido neste Termo de Referência.

3.1.5.2. Para efeitos de atendimento às dúvidas e relatos de incidentes, entende-se por usuário, as pessoas que forem indicadas pelo SENAI-SP à CONTRATADA.

3.1.5.3. O chamado deve conter a descrição sucinta do problema ou dúvida, nome e telefone do responsável pelo acompanhamento do serviço. O responsável pela abertura do chamado poderá ainda anexar ao chamado documentos ou imagens que auxiliem da identificação do problema.

3.1.5.4. Os usuários deverão homologar os chamados no prazo de 24 (vinte e quatro) horas úteis após a sua resolução pela CONTRATADA.

3.1.5.5. O prazo de solução dos chamados não deverá exceder 08 (oito) horas, podendo ser prorrogado, a critério do SENAI-SP, caso a CONTRATADA apresente, tempestivamente, razões de justificativa que comprovem a ocorrência de fatos que fogem ao controle da CONTRATADA e impedem a solução do chamado no tempo estabelecido.

3.1.6. **Avaliação dos serviços de sustentação:**

3.1.6.1. Os serviços serão avaliados em reuniões de fechamento mensal e, a critério do SENAI-SP, em reuniões extraordinárias convocadas especificamente para esse fim. A avaliação levará em consideração os indicadores e metas estabelecidos e alcançados, bem como o cumprimento das demais exigências contratuais.

3.1.6.2. Nas reuniões de avaliação serão discutidos aspectos relacionados à qualidade dos serviços e serão formuladas recomendações técnicas, administrativas e gerenciais para a melhoria contínua da qualidade dos serviços.

3.2. Suporte ao Usuário

3.2.1. A CONTRATADA deverá disponibilizar serviço de Service Desk especializado, na modalidade 8x5x365" (oito horas por dia, cinco dias úteis por semana, ao longo do ano, iniciando o atendimento entre 8h e 10h da manhã, no horário oficial de Brasília.

3.2.2. Este serviço se comportará como o centralizador das comunicações entre o SENAI-SP e a CONTRATADA, cabendo ao Service Desk prestar atendimento em primeiro nível para todas as perguntas, solicitações, reclamações, gerenciamento do ciclo de vida do incidente (encaminhar as demandas e certificar-se do atendimento) e comunicação de ocorrência de qualquer evento relacionado aos serviços prestados.

3.2.3. Entende-se por usuários para efeitos de abertura de chamados no Service-Desk, as pessoas que forem indicadas pelo SENAI-SP à CONTRATADA.

3.2.4. Os chamados poderão ser feitos por linhas telefônicas de tarifa compartilhada nas capitais e regiões metropolitanas (por exemplo 4001, 4002, 4004) e 0800 nas demais localidades ou e-mail ou extranet e deverão ter procedimentos de priorização para atendimento.

3.2.5. Relatórios mensais de acompanhamento das solicitações deverão ser disponibilizados, com informações de status, histórico e solução apresentada.

3.2.6. A CONTRATADA deverá manter um banco de dados de soluções, contendo histórico do problema ocorrido, aplicativos, hardware e software envolvidos, tentativas de soluções e a solução final.

3.2.7. O prazo de solução do incidente será em horas corridas, contadas do momento da sua detecção pela CONTRATADA ou do momento da abertura do chamado, o que ocorrer primeiro, até a sua completa resolução e restabelecimento do fornecimento do serviço, conforme níveis de serviço do item 3.1.5.5.

3.2.8. Todo chamado será registrado na Central de Atendimento e será classificado e encaminhado em sua solução segundo sua categoria e propósito.

4. Requisitos Técnicos

4.1. **Requisitos Gerais:**

4.1.1. A solução deverá fornecer uma plataforma hiper-realista de treinamento e simulação de segurança cibernética.

4.1.2. O sistema deverá simular infraestrutura de redes, tráfego de rede e cenários de ataque em redes, visando treinar e avaliar estudantes, profissionais de segurança, procedimentos e tecnologias em um ambiente seguro e controlável.

4.1.3. O sistema fornecerá uma rede virtual que emula uma rede corporativa com funcionalidades diversificadas e de forma flexível a mudanças e novas adaptações.

4.1.4. O ambiente de treinamento do sistema deverá incluir cenários de ataque previamente desenvolvidos e prontos para uso, bem como, permitir o desenvolvimento de novos cenários personalizados que serão simulados em um ambiente isolado.

4.1.5. O sistema fornecerá um catálogo de cenários de ataques de segurança cibernéticos que, através de scripts, possam ser pré-configurados, automatizados e repetitivos.

4.1.6. O ambiente de treinamento do sistema de simulação deve permitir ser facilmente resetado para um estado inicial padrão antes de uma nova sessão de treinamento.

4.1.7. O sistema deverá fornecer virtualização e emulação de dispositivos e protocolos de rede, incluindo: componentes de segurança, equipamentos de rede, servidores e aplicações de rede, dispositivos finais de usuário de rede.

4.1.8. O sistema deverá incluir um catálogo de cenários de ataques de segurança cibernética com perfil defensivo em ambiente de Tecnologia da Informação pré-configurados e prontos para uso. Uma parte dos cenários deve ser para aplicação à indivíduos em pequenas redes e outra parte dos cenários deve ser para aplicação à treinamento de equipes em uma rede completa.

4.1.9. O sistema deverá incluir um catálogo de cenários de ataques de segurança cibernética com perfil ofensivo em ambientes de Testes de Penetração pré-configurados e prontos para uso.

4.1.10. O sistema deverá fornecer um segmento de rede que permita a simulação ataques de segurança cibernética à Sistemas de Controle industriais (Industrials Control Systems – ICS) e infraestruturas críticas. Este segmento de rede deverá incluir dispositivos ICS, incluindo Controladores Lógicos Programáveis (Programmable Logic Controllers – PLC) e dispositivos de Interface Homem-Máquina (Human-Machine Interfaces - HMI).

4.1.11. O sistema deverá suportar o treinamento simultâneo de turmas independentes, sobre uma única arquitetura.

4.1.12. O sistema deverá fornecer a opção de treinamento remoto fazendo uso de conexões de Rede Privativas Virtuais (Virtual Private Networks – VPN).

4.1.13. O sistema deverá fornecer a opção para modificar a topologia da rede existente dos cenários de simulação ou criar de redes virtuais.

4.1.14. O sistema deverá fornecer uma ferramenta que permita a personalização simplificada de cenários de ataques existentes e para criar cenários de ataque de segurança cibernética.

4.1.15. O sistema deverá permitir que os participantes possam realizar o processo de autoavaliação através de um mecanismo automático de pontuação sobre o reconhecimento das atividades realizadas nos cenários de simulação, visando informar automaticamente as conquistas alcançadas por cada um dos participantes do treinamento.

4.2. **Rede Virtual**

4.2.1. O sistema deverá permitir o acesso via Internet pelos usuários finais (possibilitar o acesso remoto e realização de cursos online).

4.2.2. O sistema deverá incluir vários segmentos de sub-redes IP, VLANs e DMZ - para representar realisticamente uma rede corporativa operacional.

4.2.3. O sistema deverá incluir um gerador de tráfego para simular o tráfego usual de uma rede corporativa operacional, para maximizar a eficácia das sessões de treinamento. O gerador de tráfego precisa simular o tráfego de aplicações de rede, incluindo, no mínimo, os protocolos IP, HTTP, SMTP, POP, FTP e ICMP.

4.2.4. O sistema precisa permitir a configuração da origem e o destino do tráfego gerado pelo gerador de tráfego de rede.

4.2.5. O sistema precisa permitir a configuração do protocolo e do tipo de tráfego gerado pelo gerador de tráfego de redes.

4.2.6. O sistema precisa permitir a configuração da duração do tráfego gerado pelo gerador de tráfego de redes.

4.2.7. O sistema precisa permitir a configuração da quantidade de tráfego de rede gerada pelo gerador de tráfego de redes, permitindo a criação de grupos de fluxos de tráfego.

4.2.8. O sistema incluirá um gerador de ataque que simulará cenários de ataques de segurança cibernéticos.

4.2.9. O gerador de ataque deverá simular cenários de ataque que possa injetar código de software malicioso (malwares) na rede simulada, originada em vários segmentos de rede, de acordo com a configuração do cenário de ataque. Origens de ataque podem ser: externo (simulando uma ameaça externa) ou interno (simulando erros de configuração do usuário, erros do usuário ou invasores maliciosos).

4.2.10. O sistema deverá incluir um dispositivo de segurança do tipo “firewall de perímetro” e um outro “firewall interno”, que seja totalmente operacional e licenciado e que não seja de código aberto "open source".

4.2.11. O sistema deverá incluir um servidor de monitoramento e análise de servidores centrados em aplicações que permita monitorar o status dos serviços de todos os servidores num único conjunto de servidores através de uma interface de usuário inteligente e personalizada que possa fornecer identificação e resolução automatizadas de causas raiz de problemas.

4.2.12. O sistema deverá incluir um produto do tipo Gerenciador de Eventos e Informações de Segurança (SIEM – Security Information and Event Management) comercialmente licenciado visando simular um ambiente real de um Centro de Operações de Segurança (Security Operations Center – SOC). Este SIEM deve ser um produto comercial e não deve ser de código aberto.

4.2.13. O SIEM deverá ser pré-configurado visando incluir conjuntos de regras que suportarão os cenários de ataque para que os alertas do SIEM sejam acionados de acordo com o cenário do treinamento a ser executado.

4.2.14. O sistema deverá incluir um servidor controlador de domínio em conformidade com o padrão X.500.

4.2.15. O sistema deverá incluir um servidor de retransmissão de e-mail (SMTP Mail Relay Server).

4.2.16. O sistema deverá incluir um servidor de atribuição dinâmica de endereçamento IP (Dynamic Host Configuration Protocol – DHCP).

4.2.17. O sistema deverá incluir um segmento da topologia da rede dedicado à hospedagem, no mínimo, dos seguintes Servidores: banco de dados SQL, Controlador de Domínio, DHCP, e-Mail e Arquivos.

4.2.18. O sistema deverá incluir um segmento da topologia da rede dedicado a usuário com estações de trabalho que executem o sistema operacional Ubuntu e o sistema operacional Windows.

4.2.19. O sistema deverá incluir um segmento da topologia da rede dedicado à publicação de serviços Web, incluindo um servidor de aplicativos FTP, um servidor Web de código aberto e um servidor Web proprietário.

4.2.20. O sistema deverá incluir um segmento da topologia da rede dedicado ao acesso remoto por VPN. As estações de treinamento se conectarão à rede do treinamento por meio do servidor VPN que reside neste segmento.

4.2.21. O sistema deverá prestar suporte ao treinamento remoto por meio do uso de um aplicativo baseado em navegador WEB, sem ter que ser necessário a instalação de um software cliente na estação de treinamento.

4.2.22. O sistema deverá incluir um segmento da topologia da rede dedicado à publicação de serviços de um Provedor de Serviço da Internet (Internet Service Provider – ISP) visando simular uma rede da Internet, o qual deverá incluir um servidor de resolução de nomes (Domain Naming Services - DNS), um servidor Web proprietário e um servidor de Email Webmail de código aberto.

4.2.23. O sistema deverá incluir um segmento da topologia da rede dedicado a um ambiente industrial ICS de aplicações críticas. Deverá ainda incluir o hardware para simular processos de Tecnologia Operacional (Operational Technology – OT), os quais serão simulados em cenários de treinamento de segurança cibernética sobre OT.

4.2.24. O sistema deverá incluir segmentação da rede por VLAN e IP dos seus vários segmentos de rede (Usuários, Servidores, SIEM, ISP, VPN, ICS) para manter uma estrutura de rede que se assemelhe a uma rede corporativa real.

4.2.25. O sistema deverá permitir que o segmento de rede industrial ICS possa ser representado de forma gráfica visual por uma interface gráfica do usuário (Graphical User Interface – GUI) de um processo industrial.

4.2.26. O segmento da rede industrial ICS deve suportar um firewall com sistema de detecção de intrusão industrial (ICS Intrusion Detection System – ICS IDS), incluindo uma GUI para o fornecimento de um painel de alerta.

4.2.27. O sistema deverá incluir um IDS ICS comercial para permitir que os participantes pratiquem o monitoramento do segmento ICS. O IDS precisa ser integrado ao SIEM da rede e enviar alertas como parte dos cenários gerais de OT. O IDS ICS deverá ser um produto comercial licenciado.

4.3. **Interface de Gerenciamento do Instrutor**

4.3.1. O sistema fornecerá um console de gerenciamento ao Instrutor visando rastrear e manter um formulário de desempenho de cada participante. Cada participante será identificado, no mínimo, por um código identificador, fotografia e função. E este console deve permitir ainda a adição de campos adicionais de identificação dos participantes, se necessário.

4.3.2. O console de Gerenciamento do Instrutor fornecerá uma Interface Gráfica (GUI) intuitiva, permitindo que os instrutores configurem e executem sessões de treinamento.

4.3.3. O Console de Gerenciamento do Instrutor deverá fornecer de forma simples a configuração de uma sessão de treinamento, incluindo a seleção dos participantes, seleção da rede e a seleção do cenário de ataque.

4.3.4. O Console de Gerenciamento do Instrutor deverá fornecer a opção de gravar e permitir a reprodução das atividades realizadas pelas telas das estações de trabalho dos participantes durante uma sessão de treinamento.

4.3.5. O Console de Gerenciamento do Instrutor deverá fornecer uma função de envio de mensagem, permitindo que o Instrutor e os Participantes troquem mensagens durante uma sessão de treinamento.

4.3.6. O recurso de envio de mensagens do Console de Gerenciamento do Instrutor deverá manter registro das conversas entre Instrutor e Participantes e tais conversar poderão ser reproduzidas após a sessão para fins de revisão, esclarecimento e feedback.

4.3.7. O Console de Gerenciamento do Instrutor deverá fornecer a opção de registrar em banco de dados as sessões de treinamento e procurar sessões anteriores.

4.3.8. O Console de Gerenciamento do Instrutor deverá permitir que o Instrutor possa iniciar os cenários de ataques a qualquer instante durante uma sessão de treinamento.

4.3.9. O Console de Gerenciamento de Instrutor deverá permitir o rastreamento e classificação do desempenho do Participante.

4.3.10. O Console de Gerenciamento de Instrutor deverá fornecer a opção de executar, controlar e monitorar o fluxo em tempo real de uma sessão de treinamento.

4.3.11. O Console de Gerenciamento de Instrutor deverá fornecer um módulo de avaliação - por Participante individual e por equipe. A avaliação apoiará um mecanismo de bonificação dos Participantes.

4.3.12. O Console de Gerenciamento de Instrutor deverá fornecer a opção de armazenar e executar as lições anteriores de uma sessão de treinamento.

4.3.13. O Console de Gerenciamento de Instrutor deverá fornecer a opção de replicar uma lição anterior de uma sessão de treinamento, incluindo suas configurações e de reutilizá-las como uma nova sessão de treinamento.

4.3.14. O Console de Gerenciamento de Instrutor deverá fornecer uma visão do histórico das sessões de treinamento já realizadas.

4.3.15. O Console de Gerenciamento de Instrutor deverá exibir o detalhamento das metas e o fluxo de trabalho planejados para cada cenário das sessões de treinamento a serem executada.

4.3.16. O Console de Gerenciamento de Instrutor deverá fornecer a opção de editar as metas e o fluxo de trabalho dos cenários existentes.

4.3.17. O Console de Gerenciamento de Instrutor deverá fornecer a opção de alterar o nível de dificuldade do cenário e simular invasores mais sofisticados, modificando parâmetros como a alteração da duração do ataque, a exclusão de logs durante o ataque e a execução de um ataque silencioso.

4.3.18. O Console de Gerenciamento de Instrutor deverá fornecer uma visualização das informações da topologia da rede de treinamento em um formato diferentes formatos, como, no mínimo: JPEG, CSV, entre outros.

4.3.19. O Console de Gerenciamento de Instrutor exibirá uma linha do tempo da sessão de treinamento, exibindo os marcos dos seguintes eventos: tráfego de rede, progresso do ataque, resultados alcançados pelos participantes, anotações e mensagens.

4.3.20. A linha do tempo do Console de Gerenciamento de Instrutor também monitorará e exibirá os eventos do SIEM.

4.3.21. O cronograma do Console de Gerenciamento de Instrutor deverá fornecer um resumo de todos os eventos de treinamento na linha do tempo.

4.3.22. O Console de Gerenciamento de Instrutor permitirá que o Instrutor adicione comentários de texto que aparecerão na linha do tempo.

4.3.23. O Console de Gerenciamento de Instrutor permitirá a reprodução de uma sessão gravada, incluindo a reprodução de vídeo das telas do Participante, bem como da linha do tempo, incluindo os eventos da sessão, os marcos alcançados e os comentários. O console permitirá pular para esses eventos para uma reprodução mais rápida e objetiva daquilo que se pretende revisar.

4.3.24. O Console de Gerenciamento de Instrutor deverá fornecer a opção de ampliar a tela do Participante durante uma sessão em curso ou durante a reprodução de uma sessão de treinamento, além de permitir a ampliação para o tamanho de tela inteira, para melhorar a qualidade do acompanhamento e esclarecimento do que estiver sendo monitorado.

4.3.25. O Console de Gerenciamento de Instrutor deverá fornecer uma opção para visualizar o progresso da linha do tempo como absoluto ou relativo durante uma sessão de treinamento.

4.3.26. O Console de Gerenciamento de Instrutor permitirá que o Instrutor avance para momentos de interesse na linha do tempo durante a reprodução, incluindo marcos de ataque, conquistas de trainees e mensagens enviadas.

4.3.27. O Console de Gerenciamento de Instrutor deverá fornecer uma interface de avaliação para classificar os participantes e adicionar comentários.

4.3.28. O Console de Gerenciamento de Instrutor deverá registrar em vídeo as atividades que estiverem sendo realizadas nas telas das Estações de trabalho dos Participantes. O instrutor poderá visualizar todas as telas dos Participantes simultaneamente e ampliar a tela de um participante em específico para tela cheia.

4.3.29. O sistema deverá incluir uma Estação de Observador permitindo que tomadores de decisão, como executivos de negócios, visualizem uma exibição de alto nível do ataque, incluindo os logs de ataque, entendam o processo do ataque e como ele foi mitigado.

4.3.30. A aplicação do Instrutor deve fornecer uma indicação se uma meta foi automaticamente detectada pelos participantes. O Instrutor pode ainda editar e reescrever o feedback do sistema sobre essas metas.

4.3.31. A aplicação do Instrutor deve permitir que o Instrutor decida quando publicar um Questionário de Conhecimento (Quiz) aos Participantes, a qualquer momento durante uma sessão

de treinamento, fazendo com que os participantes possam receber uma indicação de que neste momento o Quiz já está disponível para eles.

4.3.32. A aplicação do Instrutor deve permitir que sejam adicionadas perguntas ao Questionário de Conhecimento (Quiz).

4.3.33. O Instrutor deverá ter o controle de todas as ações e do que está sendo realizadas por todos os participantes a partir de uma única console de gerenciamento.

4.3.34. O Instrutor deverá poder criar várias sessões de treinamento individuais simultaneamente, cada uma com uma topologia de rede e cenários de ataques individuais.

4.4. **Interface do Participante**

4.4.1. Os Participantes deverão conseguir treinar e praticar suas atividades sobre as ferramentas de segurança comerciais, ferramentas de investigação e monitoramento, incluindo: SIEM, Firewall, registros de eventos de Estações e Servidores, Servidores de Monitoração, Emuladores de Terminal e Analisadores de Protocolos (Sniffers) para investigação.

4.4.2. Embora a tela dos Participantes se assemelhe a uma estação de trabalho SOC da vida real, ela deverá incluir, para fins educacionais, uma Interface de Usuário de sobreposição mostrando informações de rede, plano de endereços IPs das Estações e Servidores e credenciais de acesso que permitam-no acessar e diagnosticar os equipamentos ativos de rede.

4.4.3. A tela do Participante deverá exibir o progresso do tempo e sua pontuação na sessão de treinamento em execução de forma sobreposta, sem interferir na real Interface de Usuário do produto de segurança que estiver sendo acessada.

4.4.4. A interface do Participante deverá fornecer acesso à tela da máquina virtual de todas as Estações e Servidores da rede.

4.4.5. A interface do Participante deverá fornecer uma conexão à área de trabalho remota de todas as máquinas com sistema operacional proprietário da rede.

4.4.6. A aplicação dos Participantes deverá incluir uma ferramenta de investigação interativa, onde eles poderão adicionar seus insights e evidências sobre o cenário de ataque que estão investigando.

4.4.7. A ferramenta de investigação na aplicação dos Participantes deverá fornecer uma indicação se as evidências que foram adicionadas pelo participante durante a sessão do treinamento estão corretas ou não, para que o participante possa usá-lo para aprender, consertá-lo e obter feedback em tempo real, visando ser útil para autoaprendizagem e compreensão profunda.

4.4.8. A aplicação dos Participantes deverá permitir a realização de um Quiz, objetivando testar e verificar a compreensão do participante sobre as atividades realizadas do cenário, de forma que as respostas corretas devem afetar a pontuação total do treinamento.

4.4.9. O Quiz deverá poder ser personalizado, para que novas perguntas possam ser adicionadas e as perguntas existentes possam ser removidas ou alteradas.

5. Cenários de Ataques de Segurança Cibernética

5.1. O sistema deverá incluir um gerador de ataque que simulará cenários de ataque pré-configurados. O sistema não exigirá recursos humanos ou equipes de profissionais em especializados em segurança cibernética para operar e executar os ataques, garantindo que os ataques sejam consistentes e repetíveis, minimizando, assim, a necessidade de recursos adicionais.

5.2. O sistema deverá fornecer um catálogo de ataques de segurança cibernética defensivos sobre o ambiente de Tecnologia da Informação.

5.3. O sistema deverá suportar vários níveis de dificuldade e complexidade dos cenários de ataques de segurança cibernética.

5.4. Os cenários simulados de ataque cibernético incluirão um amplo conjunto de vetores de ataque, incluindo, no mínimo: Web, E-mail, Dispositivos Móveis de Armazenamento infectados (CDs, Flash Pendrives), FTP e VPN.

5.5. O sistema deverá simular vários cenários de ataques cibernéticos de exploração, como, no mínimo: roubo de dados, rastreamento da Web, injeção de SQL, varredura de portas, varredura de PING, força bruta de senha, backdoor scripting, falsificação de sites, spear phishing, fuzzing de protocolo SSH, DNS poisoning e VPN HeartBleed.

5.6. O sistema deverá fornecer cenários de ataques cibernéticos com alto impacto tangível na rede, incluindo, no mínimo: Negação de serviço (DoS), roubo de informações e desfiguração de Websites.

5.7. O sistema deverá fornecer cenários de ataque cibernético utilizando registro de eventos (Logs) de: sistemas operacionais abertos e proprietários, SIEM, Firewall, Servidores de Monitoração, Retransmissão de e-mail, engenharia reversa, banco de dados SQL, IDS SCADA e análise forense de rede e de servidores Web.

5.8. O sistema deverá fornecer um módulo para personalização dos ataques de segurança cibernética, incluindo, no mínimo: a definição de alertas em ferramentas de segurança como silenciosos ou ativos. Isso será necessário visando modificar o nível de dificuldade dos processos diagnósticos.

5.9. O sistema deverá fornecer no módulo para personalização de ataques, no mínimo, as seguintes atividades:

i) Um controle a velocidade de execução do cenário (lenta, média, rápida);
ii) Excluir Logs criados durante um ataque, visando impactar a dificuldade dos processos diagnósticos;
iii) Alterar o endereço IP do invasor durante as ações de ataque;

iv) Adicionar scripts personalizados e integrar os scripts criados pelo usuário para propagar ataques especializados dentro do fluxo dos ataques do cenário.

5.10. O sistema deverá incluir um cenário de ataque cibernético sobre o ambiente industrial ICS usando a vulnerabilidade de conexão de site-à-site.

5.11. O sistema deverá fornecer um catálogo de ataques de segurança cibernética sobre o ambiente de Tecnologia Operacional (OT).

5.12. O sistema deverá fornecer cenários de ataques cibernéticos mostrando o impacto na rede industrial de Tecnologia Operacional (OT) como adulteração e interrupção do processo SCADA e tempo de inatividade.

5.13. O sistema deverá fornecer um cenário de ataque cibernético em ambiente industrial ICS no qual o vetor de ataque deva ser iniciado na rede de TI e atravessa para a rede OT, simulando a evolução de um ataque OT típico.

5.14. O sistema deverá fornecer conteúdo individual, incluindo cenários e redes, com foco em disciplinas específicas, tais como, no mínimo, análise de Malware, resposta a incidentes avançada, entre outros.

5.15. O sistema deverá incluir um cenário dedicado para Testadores de Penetração (PenTesters) e Ethical-Hackers. Os cenários devem incluir uma rede que possibilitem a atividade de Captura de “Bandeira” (Capture the Flag) que os Participantes devem realizar durante o treinamento. Para tanto, os Participantes podem usar o sistema operacional aberto especializado neste tipo de atividade, como o Kali Linux, para execução deste tipo de ataque.

6. Entregáveis

6.1. O sistema será fornecido com todos os componentes de hardware simulados, incluindo: storages, servidores, switches Ethernet, roteadores, Firewall, WAF, conexões, servidor tipo SCADA, servidor tipo CLPs e portas de E/S.

6.2. O sistema será fornecido com todos os componentes de software, incluindo sistemas operacionais abertos e proprietários; Suíte de aplicativos de produtividade de escritório (processador de texto, planilha eletrônica, banco de dados, exibirão de apresentações, entre outros); Servidor de Monitoração; Plataforma integrada e centralmente gerenciada de proteção de endpoints; SIEM; Firewall; Servidor de Virtualização.

6.3. O sistema deverá ser fornecido com, no mínimo, a entrega dos seguintes serviços:

i) Suporte remoto para instalação e configuração do sistema;
ii) Treinamento remoto para capacitar os Instrutores;
iii) Suporte remoto para manutenção, identificação e solução de problemas; e
iv) Garantia de Software.

6.4. O sistema deverá ser provido de documentação com seu guia de administração geral.

6.5. O sistema deverá ser provido de documentação para uso dos Instrutores contendo guia com todos os cenários e suas respectivas instruções específicas sobre os objetivos, como estão estruturados e como resolver cada cenário, além do guia incluindo visão geral da rede, nomes de usuários e senhas.

6.6. O sistema deverá fornecer apresentações aos Instrutores, que constem a documentação dos cenários, para fins de momentos, tanto inicial de instrução, quanto finais de feedback.

6.7. O sistema deverá ter cenários de exercícios tipo Capture The Flag customizáveis com painel de acompanhamento de evolução dos alunos, on line, em grupo e individuais e resultado final.

6.8. O sistema deve ter cenário do tipo wargame (blue team x red team) com dashboard de evolução on line.

7. A Arquitetura do Sistema Incluirá os Seguintes Elementos

7.1. Servidor físico para executar os componentes de software e virtualização da solução.

7.2. A arquitetura deverá permitir a conexão opcional da Estação de Trabalho de Participante via conexão VPN a partir de uma rede externa.

7.3. A arquitetura deverá incluir um segmento industrial ICS OT com PLCs e IHMs.

8. Experiência do Provedor da Solução

8.1. O provedor deve comprovar que fornece ou forneceu sistemas de treinamento operacional a organizações militares ou governamentais.

8.2. O provedor deve comprovar que fornece ou forneceu sistemas de treinamento operacional a Institutos de Ensino Superior no Brasil.

8.3. Apresentar certificado de cadastramento no DEPARTAMENTO DE PRODUTOS DE DEFESA – DEPROD – Ministério da Defesa.

ANEXO II – REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Requisitos de Segurança da Informação

1.1. As disposições abaixo são aplicáveis a qualquer objeto de contratação, onde são fornecidos serviços, sistemas, plataformas de trabalho ou qualquer outro objeto que faça uso ou seja viabilizado através de meios tecnológicos e/ou computacionais.

1.2. A aplicação dos itens deve ser avaliada diante do contexto de fornecimento e requisitos do objeto descrito na minuta de edital, descartando-se requisitos deste que não sejam pertinentes ou associados ao objeto hora contratado.

1.3. Motivada pela evolução das ameaças e riscos à Segurança da informação e Privacidade, a CONTRATANTE poderá apresentar novos requisitos de segurança durante o fornecimento do objeto contratado ou serviço prestado, trazendo a razoabilidade como fundamento para esta adequação.

1.4. Segurança Camada da Aplicação

1.4.1. A plataforma deverá conter Termo de Uso de Usuário Final, contendo as informações sobre os serviços prestados, condições de uso, privacidade, coleta e processamento de dados pessoais e sensíveis, refletindo diretrizes definidas pelo SESI-SP E SENAI-SP.

1.4.2. O sistema deverá possuir processo de exclusão dos dados (pessoais ou sensíveis) coletados a pedido do cliente e em alinhamento com regras estabelecidas pelo SESI-SP e SENAI-SP. Ressalvo nos casos que a lei exige a guarda obrigatória.

1.4.3. A arquitetura de sistema deverá ser concebida ao menos em duas camadas, separando a camada de dados da camada de front-end. A camada de front-end é entregue de modo que o usuário não consiga identificarem qual linguagem o sistema foi desenvolvido.

1.4.4. Deverá ser feita sanitização de entrada de dados em todos os campos. O código deverá ser escrito conforme melhores práticas da OWASP (Open Web Application Security Project).

1.4.5. A aplicação deverá registrar informações sobre quem se conectou na aplicação, bem como quem fez o que e quando. Os registros deverão ser armazenados por 6 meses. Quem (Credencial e IP), quando (dia/hora/minutos padrão UTC), o que foi acessado (sistema/banco/tabela/registro) e o tipo de transação (remoção/modificação/leitura)."

1.4.6. A aplicação deverá possibilitar a implantação de políticas de senha, conforme seguem:

a) Após 5 (cinco) tentativas inválidas de autenticação nos sistemas, o perfil deve ser bloqueado.
b) A reutilização de senhas obedecerá ao ciclo mínimo de 2(duas) trocas, ou seja, as últimas duas senhas não poderão ser reutilizadas.
c) As senhas deverão ter no mínimo 8 dígitos.

d) Na criação ou troca de senhas, devem ser adotadas senhas fortes.
e) A aplicação deverá possuir mecanismo de duplo fator e autenticação, compatível com o Office 365.

1.4.7. O sistema deverá possuir a capacidade de enviar e-mail “SMTP Relay”, contemplando mecanismo de autenticação.

1.4.8. Os sistemas deverão funcionar sem a necessidade do parent path habilitado.

1.4.9. O sistema não deverá possuir “Maintenance Hook”.

1.5. Requisitos Gerais de Segurança da Informação para Provedor de Nuvem

1.5.1. Caso a solução seja hospedada em provedores de nuvem, os envolvidos deverão no mínimo, possuir as certificações de conformidade com as seguintes normas:

a) ISO 27.017 – Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27.002 para serviços em nuvem.
b) ISO 27.018 – Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII.

1.6. Hospedagem das Aplicações em Nuvem ou Datacenter

1.6.1. O provedor de Nuvem ou Datacenter não deverá hospedar dados em países cujo acesso aos mesmos pode ser feito pelo governo local sem a necessidade de autorização do proprietário ou mandado judicial.

1.6.2. No contrato de prestação de serviços não poderá conter uma cláusula apontando o provedor de Nuvem ou Datacenter como dono da informação.

1.6.3. Somente poderão ser contratados provedores de nuvens cujo contrato especifique foro Brasileiro para resolução de questões judiciais.

1.6.4. O provedor de Nuvem ou Datacenter deve ter certificações reconhecidas no mercado que ateste suas premissas básicas de segurança: climatização, controle de acesso, sistema de combate ao incêndio a gás F-200, cabeamento estruturado, instalações e proteções elétricas adequadas e demais boas práticas de mercado.

1.6.5. O provedor de serviço de Nuvem ou Datacenter deverá utilizar ferramenta de backup, que possibilite a implementação da política de retenção abaixo, bem como o download de todos os dados nela armazenados. Política de retenção:

a) Diário: últimos 5 dias;
b) Semanal: últimas 5 semanas;
c) Mensal: últimos 12 meses;
d) Anual: últimos 5 anos.

1.6.6. O provedor de Nuvem ou Datacenter deverá possibilitar o controle e gerenciamento de portas de comunicação do protocolo de rede TCP/IP.

1.6.7. O provedor de Nuvem ou Datacenter deverá possuir serviço de Antivírus para os ativos de informação nas nuvens.

1.6.8. O provedor de Nuvem ou Datacenter deverá possuir serviço de IPS (Intrusion Prevention System) para os ativos de informação nas nuvens.

1.6.9. O provedor de Nuvem ou Datacenter deverá possuir serviço de WAF (Web Application Firewall) baseado no padrão OASP versão 1, 2 e 3 para os ativos de informação nas nuvens.

1.6.10. O provedor de Nuvem ou Datacenter deverá possuir serviço contra-ataques de negação de serviço distribuído.

1.6.11. O provedor do serviço de Nuvem ou Datacenter deverá apresentar relatórios mensais cobrindo os principais pontos sobre o serviço, como ataques bloqueados, disponibilidade do ambiente e demais pontos relevantes conforme escopo do contrato.

1.6.12. Somente responsável pela implantação, administração ou seus superiores, indicados pelo SESI-SP E SENAI-SP, poderão autorizar a inclusão de uma conta com "privilégios administrativos" na plataforma.

1.6.13. A plataforma deverá permitir ao SESI-SP E SENAI-SP a utilização de scanner de vulnerabilidade não intrusivo, tendo como principal objetivo identificação vulnerabilidades na aplicação.

1.6.14. A plataforma deverá disponibilizar relatórios mensais cobrindo os principais pontos sobre o serviço, como ataques bloqueados, disponibilidade do ambiente e demais pontos relevantes conforme escopo do contrato.

1.6.15. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos da informação imprescindíveis ao pleno desempenho de suas atividades.

1.7. Direitos de Propriedade da Base de Dados

1.7.1. Toda informação gerada ou transformada pelas Contratantes nos recursos computacionais da Contratada é de propriedade única e exclusiva do SESI-SP E SENAI-SP.

1.7.2. No encerramento do contrato a Contratada deverá entregar todas as informações de propriedade das Contratantes em meio eletrônico, em formato a ser definido pelo SESI-SP E SENAI-SP, tais como scripts, configurações, procedimentos, relatórios de melhoria de serviço e acompanhamento de ações realizadas na vigência do contrato, de modo a

permitir a correta migração dos serviços para outro ambiente de infraestrutura de Cloud Computing.

1.7.3. Toda a base de dados de soluções de Atendimento Técnico, contendo todos os históricos e procedimentos deverão ser disponibilizados pela Contratada às Contratantes em formato padrão e com a sua estrutura de dados.

1.7.4. Ao término do contrato todos os dados deverão ser excluídos, das plataformas da Contratada.

1.8. Sigilo das Informações

1.8.1. Guardar sigilo dos dados a que tiver acesso ou que vierem a ser compartilhados, bem como sobre os produtos de propriedade das Contratantes, além daqueles processados e gerados no ambiente físico da Contratada, reconhecendo serem estes de propriedade exclusiva do SESI-SP E SENAI-SP, os quais não podem ser cedidos, copiados, reproduzidos, publicados, divulgados de nenhuma forma, nem colocados à disposição direta ou indiretamente, locados ou vendidos a terceiros, mesmo após o encerramento do contrato, consoante o quanto contido no Termo de Confidencialidade a ser firmado pelas partes em conjunto com o instrumento contratual;

1.8.2. Não utilizar a marca das Contratantes ou qualquer material desenvolvido pelo SESI-SP e SENAI-SP para seus produtos e programas, assim como os dados dos clientes a que tenha acesso no decorrer das atividades inerentes ao contrato, em ações desenvolvidas pela Contratada fora do âmbito de atuação do contrato;

1.8.3. Tratar em caráter de estrita confidencialidade todas as informações a que tenha acesso em função do contrato, agindo com diligência para evitar sua divulgação verbal ou escrita, ou permitir o acesso, seja por ação ou omissão, a qualquer terceiro;

1.8.4. Manter, por si, por seus prepostos e contratados, irrestrito e total sigilo sobre quaisquer dados que lhe sejam fornecidos em decorrência do contrato.

1.8.5. Todas as informações veiculadas e armazenadas e/ou trafegadas nos recursos computacionais envolvidos na presente contratação, devem ser tratadas com absoluta reserva em qualquer condição e não podem ser divulgadas ou dadas a conhecer a terceiros não autorizados, aí se incluindo os próprios funcionários, estagiários, terceiros ou parceiros das Contratantes, sem a autorização destes.

1.9. Requisitos Gerais de Segurança da Informação

1.9.1. A Contratada deverá, juntamente com seu projeto de implantação, apresentar ao SESI-SP E SENAI-SP documento contendo sua Política de Segurança da Informação conforme solicitado a seguir.

1.9.2. A Política de Segurança da Informação da Contratada deverá estar alinhada com aquela adotada pelas Contratantes e abordar no mínimo os aspectos relacionados abaixo:

a) Responsabilidades associadas a acesso, gestão e guarda de informações, estabelecidas para os profissionais integrantes dos seus quadros ou terceiros.
b) Cumprimento irrestrito da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18) e possuir conformidade com a GDPR (General Data Protection Regulation);
c) Sempre que possível, recomendado ou solicitado pela contratante, implementar o uso de criptografia e/ou certificados digitais para operação ou gerenciamento do ambiente;
d) Emprego de equipamento de firewall, em suas instalações, com suporte a VPN/IPSEC, utilizando apenas algoritmos criptográficos classificados como "uso aceitável" pelo NIST (National Institute of Standard Technology), definindo as fronteiras físicas e lógicas entre as redes das Contratantes e da Contratada e outros acessos necessários à prestação dos serviços, bem como solução de software de prevenção de intrusão (IPS) para o ambiente;
e) Utilização de softwares antivírus e de proteção a ameaças avançadas, em todos os equipamentos das suas instalações, capazes de detectar e remover vírus, cavalos de troia, warms e ameaças correlatas, com atualizações frequentes e automáticas das vacinas e novas versões contemplando todos os servidores e estações de rede. Essa solução deverá ter capacidade e performance compatível com aquela instalada e em operação no ambiente das Contratantes;
f) A Contratada deverá permitir às Contratantes o acesso local ou remoto aos seus sistemas, assim como a todo e qualquer equipamento disponibilizado na prestação dos serviços, bem como aos ambientes físicos com controle de acesso, para fins de auditoria em segurança;
g) Deverão ser adotados procedimentos de acesso seguro ambiente, permitindo inclusive a autenticação forte e utilização de múltiplos fatores de autenticação, bem como a aplicação de certificados digitais e técnicas criptográficas para armazenamento de dados;

2. Requisitos de Privacidade e Conformidade LGPD

2.1. Os requisitos de privacidade sob perspectiva da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18), serão aplicáveis quando o objeto da contratação envolva direta ou indiretamente o tratamento de dados pessoais, especialmente os categorizados como sensíveis.
2.2. Qualquer item anterior presente neste anexo ou na minuta de edital que discorra sobre mesmo tema ou definição, deve ser interpretado de forma complementar com ênfase no entendimento de melhor garantia aos direitos dos titulares dos dados e/ou maior conformidade com a legislação aplicável.
2.3. Salvo disposições contrarias específicas, os termos abaixo terão as seguintes definições:

a) **Titulares:** Pessoa física singular identificada ou identificável, a qual poderá ter seus dados pessoais tratados;

b) **Dados Pessoais:** Qualquer informação relativa a uma pessoa singular identificada ou identificável ou qualquer outra informação que se qualifica como "Dados Pessoais" nos termos das leis de proteção de Dados.

c) **Dados Sensíveis:** Qualquer informação do titular que possa revelar sua origem racial ou étnica, religião, filiação sindical, opinião política, dados referentes à saúde e vida sexual, dados genético ou biométrico.

d) **Tratamento:** Qualquer operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

e) **Controlador:** Pessoas jurídica ou estabelecimento que nos termos da lei atua como controlador das informações, determinando as finalidades, meios de tratamento e demais ações sobre os dados pessoais sob sua responsabilidade.

f) **Operador:** Pessoa natural ou jurídica que sob orientação ou determinação do Controlador, executa o processamento e tratamento de dados pessoais dos titulares;

g) **Encarregado:** Pessoa nomeada nos termos da lei para atuar como canal de comunicação entre Controlador, Operadores, Titulares, Agências Reguladoras e demais interessados e responsáveis pela operacionalização e conformidade com a LGPD.

2.4. Para efeito de delimitação de papeis e responsabilidades, neste documento a CONTRATANTE desempenhará o papel de CONTROLADOR e a CONTRATADA o papel de OPERADOR.

2.5. O OPERADOR deverá obter termo de confidencialidade dos seus colaboradores que estiverem envolvidos no tratamento dos dados em nome do CONTROLADOR, sendo esta exigência dispensada caso outro documento interno estabelecido tenha mesma aplicação e validade, por exemplo contrato de trabalho.

2.6. O OPERADOR deverá apresentar as informações do seu encarregado de proteção de dados, ou, colaborador que desempenhe atividades e responsabilidade semelhante sobre o tema, caso o OPERADOR seja dispensado de nomeação formal conforme previsão da LGPD.

2.7. O tratamento dos dados pessoais deverá ser executado de forma limitada e de acordo com as orientações e definições de finalidade determinados pelo CONTROLADOR.

2.8. De acordo com as instruções fornecidas pelo CONTROLADOR, o OPERADOR deve ajustar, excluir ou bloquear os dados processados, notificando sem atrasos se em sua opinião a instrução infringir as regulamentações aplicáveis de proteção de dados.

2.9. O OPERADOR deverá fornecer ao CONTROLADOR as informações necessárias para permitir que este cumpra as obrigações de notificação, mantenha registros das

atividades de processamento e/ou realize a avaliação de impacto da proteção de dados caso necessário.

2.10. Os dados pessoais tratados deverão ser devolvidos ao CONTROLADOR e eliminados ao final do contrato ou sob sua solicitação, exceto em situações em que legislação especifique a necessidade e condição de manutenção dos dados.

2.11. Em caso de exclusão de dados por solicitação do CONTROLADOR, fica estabelecida a necessidade do OPERADOR demonstrar que os dados foram eliminados e não poderão ser reconstruídos, evidenciando inclusive por escrito que todos que todas as mídias foram devolvidas ou destruídas. Caso haja requisitos legais vinculativos que não permitam apagar dados contratuais ou categorias de dados, o OPERADOR deverá informar o CONTROLADOR sobre tais requisitos.

2.12. O OPERADOR deverá possuir Política de Segurança e Privacidade que exponha suas diretrizes e definições sobre o tema privacidade.

2.13. É vedado ao OPERADOR a subcontratação de operadores sem previa análise e expressa autorização do CONTROLADOR.

2.14. O OPERADOR deve estabelecer programa de Segurança da Informação e privacidade baseado nos principais Frameworks de mercado, como por exemplo ISO 27001/27002/27701, NIST etc., informando ao CONTROLADOR os dados para contato do seu gestor sobre o tema.

2.15. O programa de Segurança da Informação e Privacidade do OPERADOR deverá contar com ciclo de identificação e resposta à incidentes.

2.16. O OPERADOR deverá notificar qualquer incidente de segurança, tendo prazo de 72 horas para comunicar os que envolvam ou possam impactar dados pessoais tratados em nome do CONTROLADOR.

2.17. A critério do CONTROLADOR, deverão ser coordenadas medidas técnicas e organizacionais voltadas para Segurança da Informação e Privacidade, incluindo visitas às instalações do OPERADOR para auditorias e validação das medidas estabelecidas.

2.18. O CONTROLADOR ou seus representantes têm o direito de realizar verificações em cumprimento aos requisitos deste Contrato. O OPERADOR deve fornecer as informações desejadas e, mediante solicitação do CONTROLADOR e dentro de um prazo razoável, apresentar provas documentais de que cumpriu suas obrigações, preenchendo um questionário fornecido pelo CONTROLADOR ou confirmando por escrito que as medidas acordadas são adequadas e atuais.

2.19. O OPERADOR deve notificar o responsável pelo gerenciamento do contrato do CONTROLADOR por escrito, se houver alguma alteração significativa nas medidas técnicas e organizacionais descritas. No caso de qualquer redução previsível na

efetividade da segurança, o consentimento do CONTROLADOR deve ser obtido por escrito antes que a alteração seja realizada.

2.20. O OPERADOR deverá implementar programa de treinamento e conscientização sobre Segurança da Informações e Privacidade, principalmente com temas e ações relacionadas privacidade e conformidade com a LGPD.

2.21. O OPERADOR deverá desenvolver, manter e apresentar relatório sobre brechas na segurança e proteção de dados, bem como inventário e ciclo de gestão de riscos em segurança da Informação.

2.22. O OPERADOR deve informar o CONTROLADOR sem demora sobre verificações das autoridades de supervisão que ocorrem na empresa do OPERADOR, ou na infraestrutura de TI utilizada, e onde os dados pessoais do CONTROLADOR estão sendo processados.

2.23. Na hipótese de iminente acesso aos dados do CONTROLADOR no contexto de apreensão, confisco, inquéritos judiciais ou outras ações aplicáveis por parte das autoridades, ou no contexto de procedimentos de insolvência ou outras medidas de terceiros, o OPERADOR deverá comunicar imediatamente tal situação ao CONTROLADOR.

2.24. O OPERADOR deverá informar sem demora a todas as partes envolvidas em tal ação que o poder de disposição sobre os dados sujeitos ao presente contrato está com o CONTROLADOR, não devendo transferir qualquer dado a terceiros nem permitir que terceiros tenham acesso aos dados sem a expressa autorização do CONTROLADOR.

2.25. O OPERADOR nos termos da Lei Geral de Proteção de Dados é solidário junto ao CONTROLADOR no desempenho das obrigações e cumprimento da legislação, devendo atuar ativamente para conformidade e pronta resposta.

SESI SENAI

ANEXO III - REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

Item	Análise	Evidências
1. Requisitos de Segurança da Informação		
1.1. As disposições abaixo são aplicáveis a qualquer objeto de contratação, onde são fornecidos serviços, sistemas, plataformas de trabalho ou qualquer outro objeto que faça uso ou seja viabilizado através de meios tecnológicos e/ou computacionais.		
1.2. A aplicação dos itens deve ser avaliada diante do contexto de fornecimento e requisitos do objeto descrito na minuta de edital, descartando-se requisitos deste que não sejam pertinentes ou associados ao objeto hora contratado		
1.3. Motivada pela evolução das ameaças e riscos à Segurança da informação e Privacidade,a CONTRATANTE poderá apresentar novos requisitos de segurança durante o fornecimento do objeto contratado ou serviço prestado, trazendo a razoabilidade como fundamento para esta adequação.		
1.4. Segurança na camada da aplicação		
1.4.1. A plataforma deverá conter Termo de Uso de Usuário Final, contendo as informações sobre os serviços prestados, condições de uso, privacidade, coleta e processamento de dados pessoais e sensíveis, refletindo diretrizes definidas pelo SESI-SP e SENAI-SP		
1.4.2. O sistema deverá possuir processo de exclusão dos dados (pessoais ou sensíveis) coletados a pedido do cliente e em alinhamento com regras estabelecidas pelo SESI-SP e SENAI-SP e SENAI-SP. Ressalvo nos casos que a lei exige a guarda obrigatória		
1.4.3. A arquitetura de sistema deverá ser concebida ao menos em duas camadas, separando a camada de dados da camada de front-end. A camada de front-end é entregue de modo que o usuário não consiga identificarem qual linguagem o sistema foi desenvolvido.		
1.4.4. Deverá ser feita sanitização de entrada de dados em todos os campos. O código deverá ser escrito conforme melhores práticas da OWASP (Open Web Application Security Project).		
1.4.5. A aplicação deverá registrar informações sobre quem se conectou na aplicação, bem como quem fez o que e quando. Os registros deverão ser armazenados por 6 meses. Quem (Credencial e IP), quando (dia/hora/minutos padrão UTC), o que foi acessado (sistema/banco/tabela/registro) e o tipo de transação (remoção/modificação/leitura)."		
1.4.6. A aplicação deverá possibilitar a implantação de políticas de senha, conforme seguem:		
a) Após 5 (cinco) tentativas inválidas de autenticação nos sistemas, o perfil deve ser bloqueado.		
b) A reutilização de senhas obedecerá ao ciclo mínimo de 2(duas) trocas, ouseja, as últimas duas senhas não poderão ser reutilizadas.		
c) As senhas deverão ter no mínimo 8 dígitos.		
d) Na criação ou troca de senhas, devem ser adotadas senhas fortes.		
e) A aplicação deverá possuir mecanismo de duplo fator e autenticação,compatível com o Office 365.		
1.4.7. O sistema deverá possuir a capacidade de enviar e-mail “SMTP Relay”, contemplando mecanismo de autenticação.		
1.4.8. Os sistemas deverão funcionar sem a necessidade do parent path habilitado.		
1.4.9. O sistema não deverá possuir “Maintenance Hook”.		
1.5. Requisitos gerais de Segurança da Informação para Provedor de Nuvem		
1.5.1. Caso a solução seja hospedada em provedores de nuvem, os envolvidos deverão no mínimo, possuir as certificações de conformidade com as seguintes normas:		
a) ISO 27.017 - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27.002 para serviços em nuvem		
b) ISO 27.018 - Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam comoprocessadores de PII.		
1.6. Hospedagem das aplicações em Nuvem ou Datacenter		
1.6.1. O provedor de Nuvem ou Datacenter não deverá hospedar dados em países cujo acesso aos mesmos pode ser feito pelo governo local sem a necessidade de autorização do proprietário ou mandado judicial.		
1.6.2. No contrato de prestação de serviços não poderá conter uma cláusula apontando provedor de Nuvem ou Datacenter como dono		
1.6.3. Somente poderão ser contratados provedores de nuvens cujo contrato especifique foro Brasileiro para resolução de questões		
1.6.4. O provedor de Nuvem ou Datacenter deve ter certificações reconhecidas no mercado que ateste suas premissas básicas de		
1.6.5. O provedor de serviço de Nuvem ou Datacenter deverá utilizar ferramenta de backup, que possibilite a implementação da política de retenção abaixo, bem como o download de todos os dados nela armazenados. Política de retenção:		
a) Diário: últimos 5 dias;		
b) Semanal: últimas 5 semanas;		
c) Mensal: últimos 12 meses;		
d) Anual: últimos 5 anos.		
1.6.6. O provedor de Nuvem ou Datacenter deverá possibilitar o controle e gerenciamento de portas de comunicação do protocolo de rede TCP/IP.		
1.6.7. O provedor de Nuvem ou Datacenter deverá possuir serviço de Antivírus para os ativos de informação nas nuvens.		
1.6.8. O provedor de Nuvem ou Datacenter deverá possuir serviço de IPS (Intrusion Prevention System) para os ativos de informação nas nuvens.		
1.6.9. O provedor de Nuvem ou Datacenter deverá possuir serviço de WAF (Web Application Firewall) baseado no padrão OASP versão 1, 2 e 3 para os ativos de informação nas nuvens.		
1.6.10. O provedor de Nuvem ou Datacenter deverá possuir serviço contra-ataques de negação de serviço distribuído.		
1.6.11. O provedor do serviço de Nuvem ou Datacenter deverá apresentar relatórios mensais cobrindo os principais pontos sobre o serviço, como ataques bloqueados, disponibilidade do ambiente e demais pontos relevantes conforme escopo do contrato.		
1.6.12. Somente responsável pela implantação, administração ou seus superiores, indicados pelo SESI-SP e SENAI-SP e SENAI-SP, poderão autorizar a inclusão de uma conta com “privilégios administrativos” na plataforma.		
1.6.13. A plataforma deverá permitir ao SESI-SP e SENAI-SP e SENAI-SP a utilização de scanner de vulnerabilidade não intrusivo, tendo como principal objetivo identificação vulnerabilidades na aplicação.		
1.6.14. A plataforma deverá disponibilizar relatórios mensais cobrindo os principais pontos sobre o serviço, como ataques bloqueados, disponibilidade do ambiente e demais pontos relevantes conforme escopo do contrato.		
1.6.15. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos da informação imprescindíveis ao pleno desempenho de suas atividades.		

1.7. Direitos de Propriedade da Base de Dados		
1.7.1. Toda informação gerada ou transformada pelas Contratantes nos recursos computacionais da Contratada é de propriedade única e exclusiva do SESI-SP e SENAI-SP e SENAI-SP.		
1.7.2. No encerramento do contrato a Contratada deverá entregar todas as informações de propriedade das Contratantes em meio eletrônico, em formato a ser definido pelo SESI-SP e SENAI-SP e SENAI-SP, tais como scripts, configurações, procedimentos, relatórios de melhoria de serviço e acompanhamento de ações realizadas na vigência do contrato, de modo a permitir a correta migração dos serviços para outro ambiente de infraestrutura de Cloud Computing.		
1.7.3. Toda a base de dados de soluções de Atendimento Técnico, contendo todos os históricos e procedimentos deverão ser disponibilizados pela Contratada às Contratantes em formato padrão e com a sua estrutura de dados.		
1.7.4. Ao término do contrato todos os dados deverão ser excluídos, das plataformas da Contratada.		
1.8. Sigilo das Informações		
1.8.1. Guardar sigilo dos dados a que tiver acesso ou que vierem a ser compartilhados, bem como sobre os produtos de propriedade das Contratantes, além daqueles processados e gerados no ambiente físico da Contratada, reconhecendo serem estes de propriedade exclusiva do SESI-SP e SENAI-SP e SENAI-SP, os quais não podem ser cedidos, copiados, reproduzidos, publicados, divulgados de nenhuma forma, nem colocados à disposição direta ou indiretamente, locados ou vendidos a terceiros, mesmo após o encerramento do contrato, consoante o quanto contido no Termo de Confidencialidade a ser firmado pelas partes em conjunto com o instrumento contratual;		
1.8.2. Não utilizar a marca das Contratantes ou qualquer material desenvolvido pelo SESI-SP e SENAI-SP e SENAI-SP para seus produtos e programas, assim como os dados dos clientes a que tenha acesso no decorrer das atividades inerentes ao contrato, em ações desenvolvidas pela Contratada fora do âmbito de atuação do contrato;		
1.8.3. Tratar em caráter de estrita confidencialidade todas as informações a que tenha acesso em função do contrato, agindo com diligência para evitar sua divulgação verbal ou escrita, ou permitir o acesso, seja por ação ou omissão, a qualquer terceiro;		
1.8.4. Manter, por si, por seus prepostos e contratados, irrestrito e total sigilo sobre quaisquer dados que lhe sejam fornecidos em decorrência do contrato.		
1.8.5. Todas as informações veiculadas e armazenadas e/ou trafegadas nos recursos computacionais envolvidos na presente contratação, devem ser tratadas com absoluta reserva em qualquer condição e não podem ser divulgadas ou dadas a conhecer a terceiros não autorizados, aí se incluindo os próprios funcionários, estagiários, terceiros ou parceiros das Contratantes, sem a autorização destes.		
1.9. Requisitos Gerais de Segurança da Informação		
1.9.1. A Contratada deverá, juntamente com seu projeto de implantação, apresentar ao SESI-SP e SENAI-SP documento contendo sua Política de Segurança da Informação conforme solicitado a seguir.		
1.9.2. A Política de Segurança da Informação da Contratada deverá estar alinhada com aquela adotada pelas Contratantes e abordar no mínimo os aspectos relacionados abaixo:		
a) Responsabilidades associadas a acesso, gestão e guarda de informações, estabelecidas para os profissionais integrantes dos seus quadros ou terceiros;		
b) Cumprimento irrestrito da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18) e possuir conformidade com a GDPR (General Data Protection Regulation);		
c) Sempre que possível, recomendado ou solicitado pela contratante, implementar o uso de criptografia e/ou certificados digitais para operação ou gerenciamento do ambiente;		
d) Emprego de equipamento de firewall, em suas instalações, com suporte a VPN/IPSEC, utilizando apenas algoritmos criptográficos classificados como "uso aceitável" pelo NIST (National Institute of Standard Technology), definindo as fronteiras físicas e lógicas entre as redes das Contratantes e da Contratada e outros acessos necessários à prestação dos serviços, bem como solução de software de prevenção de intrusão (IPS) para o ambiente;		
e) Utilização de softwares antivírus e de proteção a ameaças avançadas, em todos os equipamentos das suas instalações, capazes de detectar e remover vírus, cavalos de troia, warms e ameaças correlatas, com atualizações frequentes e automáticas das vacinas e novas versões contemplando todos os servidores e estações de rede. Essa solução deverá ter capacidade e performance compatível com aquela instalada e em operação no ambiente das Contratantes;		
f) A Contratada deverá permitir às Contratantes o acesso local ou remoto aos seus sistemas, assim como a todo e qualquer equipamento disponibilizado na prestação dos serviços, bem como aos ambientes físicos com controle de acesso, para fins de auditoria em segurança;		
g) Deverão ser adotados procedimentos de acesso seguro ambiente, permitindo inclusive a autenticação forte e utilização de múltiplos fatores de autenticação, bem como a aplicação de certificados digitais e técnicas criptográficas para armazenamento de dados;		

SESI SENAI	ANEXO III – Requisitos de Privacidade e Conformidade LGPD		
Item		**Análise**	**Evidências**
2 Requisitos de Privacidade e Conformidade LGPD			
2.1 Os requisitos de privacidade sob perspectiva da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18), serão aplicáveis quando o objeto da contratação envolva direta ou indiretamente o tratamento de dados pessoais, especialmente os categorizados como sensíveis.			
2.2 Qualquer item anterior presente neste anexo ou na minuta de edital que discorra sobre mesmo tema ou definição, deve ser interpretado de forma complementar com ênfase no entendimento de melhor garantia aos direitos dos titulares dos dados e/ou maior conformidade com a legislação aplicável.			
2.3 Salvo disposições contrarias específicas, os termos abaixo terão as seguintes definições:			
	a) **Titulares:** Pessoa física singular identificada ou identificável, a qual poderá ter seus dados pessoais tratados;		
	b) **Dados Pessoais:** Qualquer **informação** relativa a uma pessoa singular identificada ou identificável ou qualquer outra informação que se qualifica como "Dados Pessoais" nos termos das leis de proteção de Dados;		
	c) **Dados Sensíveis:** Qualquer informação do titular que possa revelar sua origem racial ou étnica, religião, filiação sindical, opinião política, dados referentes à saúde e vida sexual, dados genético ou biométrico;		
	d) **Tratamento:** Qualquer operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;		
	e) **Controlador:** Pessoas jurídica ou estabelecimento que nos termos da lei atua como controlador das informações, determinando as finalidades, meios de tratamento e demais ações sobre os dados pessoais sob sua responsabilidade;		
	f) **Operador:** Pessoa natural ou jurídica que sob orientação ou determinação do Controlador, executa o processamento e tratamento de dados pessoais dos titulares;		
	g) **Encarregado:** Pessoa nomeada nos termos da lei para atuar como canal de comunicação entre Controlador, Operadores, Titulares, Agências Reguladoras e demais interessados e responsáveis pela operacionalização e conformidade com a LGPD.		
2.4 Para efeito de delimitação de papeis e responsabilidades, neste documento a CONTRATANTE desempenhará o papel de CONTROLADOR e a CONTRATADA o papel de OPERADOR.			
2.5 O OPERADOR deverá obter termo de confidencialidade dos seus colaboradores que estiverem envolvidos no tratamento dos dados em nome do CONTROLADOR, sendo esta exigência dispensada caso outro documento interno estabelecido tenha mesma aplicação e validade, por exemplo contrato de trabalho.			
2.6 A OPERADOR deverá apresentar as informações do seu encarregado de proteção de dados, ou, colaborador que desempenhe atividades e responsabilidade semelhante sobre o tema, caso o OPERADOR seja dispensado de nomeação formal conforme previsão da LGPD.			
2.7 O tratamento dos dados pessoais deverá ser executado de forma limitada e de acordo com as orientações e definições de finalidade determinados pelo CONTROLADOR.			
2.8 De acordo com as instruções fornecidas pelo CONTROLADOR, o OPERADOR deve ajustar, excluir ou bloquear os dados processados, notificando sem atrasos se em sua opinião a instrução infringir as regulamentações aplicáveis de proteção de dados.			
2.9 O OPERADOR deverá fornecer ao CONTROLADOR as informações necessárias para permitir que este cumpra as obrigações de notificação, mantenha registros das atividades de processamento e/ou realize a avaliação de impacto da proteção de dados caso necessário.			
2.10 Os dados pessoais tratados deverão ser devolvidos ao CONTROLADOR e eliminados ao final do contrato ou sob sua solicitação, exceto em situações em que legislação especifique a necessidade e condição de manutenção dos dados.			
2.11 Em caso de exclusão de dados por solicitação do CONTROLADOR, fica estabelecida a necessidade do OPERADOR demonstrar que os dados foram eliminados e não poderão ser reconstruídos, evidenciando inclusive por escrito que todos que todas as mídias foram devolvidas ou destruídas. Caso haja requisitos legais vinculativos que não permitam apagar dados contratuais ou categorias de dados, o OPERADOR deverá informar o CONTROLADOR sobre tais requisitos.			
2.12 O OPERADOR deverá possuir Política de Segurança e Privacidade que exponha suas diretrizes e definições sobre o tema privacidade.			
2.13 É vedado ao OPERADOR a subcontratação de operadores sem previa análise e expressam autorização do CONTROLADOR.			
2.14 O OPERADOR deve estabelecer programa de Segurança da Informação e privacidade baseado nos principais Frameworks de mercado, como por exemplo ISO 7001/27002/27701, NIST etc., informando ao CONTROLADOR os dados para contato do seu gestor sobre o tema.			
2.15 O programa de Segurança da Informação e Privacidade do OPERADOR deverá contar com ciclo de identificação e resposta à incidentes.			
2.16 O OPERADOR deverá notificar qualquer incidente de segurança, tendo prazo de 72 horas para comunicar os que envolvam ou possam impactar dados pessoais tratados em nome do CONTROLADOR.			
2.17 A critério do CONTROLADOR, deverão ser coordenadas medidas técnicas e organizacionais voltadas para Segurança da Informação e Privacidade, incluindo visitas às instalações do OPERADOR para auditorias e validação das medidas estabelecidas.			
2.18 O CONTROLADOR ou seus representantes têm o direito de realizar verificações em cumprimento aos requisitos deste Contrato. O OPERADOR deve fornecer as informações desejadas e, mediante solicitação do CONTROLADOR e dentro de um prazo razoável, apresentar provas documentais de que cumpriu suas obrigações, preenchendo um questionário fornecido pelo CONTROLADOR ou confirmando por escrito que as medidas acordadas são adequadas e atuais.			
2.19 O OPERADOR deve notificar o responsável pelo gerenciamento do contrato do CONTROLADOR por escrito, se houver alguma alteração significativa nas medidas técnicas e organizacionais descritas. No caso de qualquer redução previsível na efetividade da segurança, o consentimento do CONTROLADOR deve ser obtido por escrito antes que a alteração seja realizada.			
2.20 O OPERADOR deverá implementar programa de treinamento e conscientização sobre Segurança da Informações e Privacidade, principalmente com temas e ações relacionadas privacidade e conformidade com a LGPD.			

2.21 O OPERADOR deverá desenvolver, manter e apresentar relatório sobre brechas na segurança e proteção de dados, bem como inventário e ciclo de gestão de riscos em segurança da Informação.		
2.22 O OPERADOR deve informar o CONTROLADOR sem demora sobre verificações das autoridades de supervisão que ocorrem na empresa do OPERADOR, ou na infraestrutura de TI utilizada, e onde os dados pessoais do CONTROLADOR estão sendo processados.		
2.23 Na hipótese de iminente acesso aos dados do CONTROLADOR no contexto de apreensão, confisco, inquéritos judiciais ou outras ações aplicáveis por parte das autoridades, ou no contexto de procedimentos de insolvência ou outras medidas de terceiros, o OPERADOR deverá comunicar imediatamente tal situação ao CONTROLADOR.		
2.24 O OPERADOR deverá informar sem demora a todas as partes envolvidas em tal ação que o poder de disposição sobre os dados sujeitos ao presente contrato está com o CONTROLADOR, não devendo transferir qualquer dado a terceiros nem permitir que terceiros tenham acesso aos dados sem a expressa autorização do CONTROLADOR.		
2.25 O OPERADOR nos termos da Lei Geral de Proteção de Dados é solidário junto ao CONTROLADOR no desempenho das obrigações e cumprimento da legislação, devendo atuar ativamente para conformidade e pronta resposta.		

ANEXO C - MODELO PROPOSTA

Processo: 3000430638 **Edital:** 000000895/2025 **Tipo:** PS - Disputa Aberta **Data:** 01.12.2025

Centro: SENAI SEDE

Grupo de Compradores: SUPERVISAO DE CONTR DE OBRAS E SERVICOS

Comprador: PAULO MOREIRA DOS SANTOS NETO **Telefone:** **E-mail:** PAULO.NETO@SESISENAISP.ORG.BR

Fornecedor: **CNPJ:**

Endereço: **E-mail Corporativo:**

CEP: **Bairro:** **Cidade:** **Estado:**

Contato: **Telefone:** **E-mail de Contato:**

LOTE - 01

ITEM	ID PRODUTO	DESCRIÇÃO	MARCA	MODELO / REFERÊNCIA	QUANT.	U.M.	VALOR UNITÁRIO	IMPOSTO *1	VALOR TOTAL	PRAZO DE ENTREGA	GARANTIA
0001	3005825	PLATAFORMA SIM. ATAQ. E DEF. CIBERNÉTICA			2	UA					
								VALOR TOTAL			

CONDIÇÕES DE PAGAMENTO	VALIDADE DA PROPOSTA	FRETE

RESPONSÁVEL PELA PROPOSTA:

OBSERVAÇÕES:

Encaminhar documento complementar (catálogo e/ou características técnicas) do material/equipamento ofertado, quando este não corresponder as especificações solicitadas.

*1 Destacar os impostos devidos, conforme objeto da cotação, se for o caso.

ESPECIFICAÇÕES TÉCNICAS:

ID Produto: 3005825 Descrição: PLATAFORMA SIM. ATAQ. E DEF. CIBERNÉTICA

3005825 - PLATAFORMA DE SIMULAÇÃO DE ATAQUE E DEFESA CIBERNÉTICA

1 - OBJETIVO:

1.1 - LICENÇA DE SOFTWARE DE SOLUÇÃO DE SIMULAÇÃO HIPER-REALISTA DE SEGURANÇA PARA ATAQUE E DEFESA CIBERNÉTICOS.

2 - CARACTERÍSTICAS:

2.1 - LICENÇA DE SOFTWARE PARA 10 USUÁRIOS SIMULTÂNEOS;

2.2 - VIGÊNCIA DE 12 MESES;

2.3 - DEMAIS CARACTERÍSTICAS CONFORME MEMORIAL DESCRITIVO E TERMO DE REFERÊNCIA.

3005825 - PLATAFORMA DE SIMULAÇÃO DE ATAQUE E DEFESA CIBERNÉTICA

RELAÇÃO DOS LOCAIS DE ENTREGA

UNIDADE: SENAI SEDE **MUNICÍPIO: SÃO PAULO - SP** **CEP: 01311-923**

ITEM	ID PRODUTO	DESCRIÇÃO	U.M.	QUANT.
0001.0001	3005825	PLATAFORMA SIM. ATAQ. E DEF. CIBERNÉTICA	UA	2,000

ANEXO D

MINUTA DE CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE FORNECIMENTO DE PLATAFORMA DE SIMULAÇÃO DE ATAQUE E DEFESA CIBERNÉTICA HIPER-REALISTA AO SENAI-SP

Pelo presente instrumento particular e, na melhor forma de direito, em que são partes, de um lado, o SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL - SENAI, Departamento Regional de São Paulo, com sede na Avenida Paulista nº 1313, 3º andar, Bairro Bela Vista, CEP 01311-923, na cidade de São Paulo, Estado de São Paulo, inscrito no CNPJ sob o nº 03.774.879/0001-02, neste ato representado pelo Diretor da Escola SENAI Paulo Antônio Skaf, CNPJ_____, ora localizada na _____, bairro, CEP, CIDADE, UF, a seguir denominado, simplesmente, SENAI-SP, e, de outro lado, , com inscrição no CNPJ sob o nº , com sede na , nº , Bairro , CEP , na cidade de , estado de , neste ato representada de acordo com seus atos constitutivos, a seguir denominada, simplesmente, CONTRATADA, têm, entre si, ajustados e contratados a celebração do presente contrato, mediante as seguintes cláusulas e condições que, mutuamente, aceitam e outorgam.

Cláusula Primeira – Do Objeto

1.1 Constitui o objeto do presente contrato a prestação de serviços pela CONTRATADA ao SENAI-SP de Fornecimento de Solução com ambiente hiper-realista para a simulação de ataques cibernéticos em sistemas de Tecnologia da Informação (TI), por meio do fornecimento de licenças no modelo SaaS (Software as a Service), nos termos do Chamamento Público – PSDA 109/2025, Memorial Descritivo e demais anexos, que passam a fazer parte integrante do presente instrumento independente de transcrição, para todos os fins e efeitos de direito.

1.2 A solução hiper-realista para a simulação de ataques cibernéticos, doravante denominada Solução de Segurança Cibernética, é um ambiente virtual que permite a simulação de ambientes de ataque e defesa cibernéticos em diversos cenários e vírus emulados.

1.3 A Solução de Segurança Cibernética deve contemplar:

a) Fornecimento de 10 (dez) licenças no modelo SaaS por, pelo menos, 12 (doze) meses de permissão de uso.
b) Pacote mínimo de 50 (cinquenta) cenários nos níveis básico, intermediário e avançado;
c) Backup e Restore;
d) Sustentação;
e) Suporte ao Usuário.

1.4 Demais Especificações do objeto encontram-se previstas no Memorial Descritivo, Anexo B, do PSDA 109/2025.

1.5 Faz parte integrante deste contrato o Regulamento para Contratação e Alienação – RCA – do Serviço Nacional de Aprendizagem Industrial – SENAI e a Proposta da CONTRATADA com data de ___/___/202___.

Cláusula Segunda – Da Vigência e Dos Prazos

2.1. Este contrato vigorará pelo período de 12 (doze) meses, a contar do dia ___/___/___ até o dia ____/____/____, podendo ser renovado por meio da elaboração de Termo Aditivo, até o limite máximo de 36 (trinta e seis) meses, observadas as demais disposições contidas no artigo 34 e 38 do RCA.

2.2. Fica convencionado que, poderá, a critério das partes, havendo prorrogação da vigência, após o 12º mês, ser aplicado o reajustamento de preço com base na variação da média aritmética simples da variação acumulada nos últimos 12 (doze) meses, do índice IPCA/IBGE, relativo ao mês anterior do término de vigência do contrato ou, mediante concordância entre as partes, referente ao segundo mês anterior ao vencimento deste instrumento, ou ainda, por outro índice que venha a substituí-los, caso haja a extinção de um deles.

Cláusula Terceira – Dos Preços e Pagamentos

3.1. O preço global a ser pago pela execução dos serviços, objeto deste contrato é no importe máximo anual de até R$ ( ), de acordo com a proposta da CONTRATADA e Anexo, I, deste contrato.

3.1.1 Serão realizados os pagamentos apenas dos serviços efetivamente realizados.
3.1.2 Os preços constantes acima são fixos e irreajustáveis pelo período de 12 (doze) meses.

3.2 Os pagamentos serão feitos a partir da validação da unidade requisitante, de acordo com a autorização para faturamento ou documento equivalente emitido pelo SENAI-SP.

3.3 Uma vez aceitos os serviços pelo SENAI-SP, a CONTRATADA deverá emitir as faturas correspondentes, individualmente para cada unidade atendida pela solução no período.

3.4 Os pagamentos serão efetuados diretamente pela Gerência Sênior Contábil e Financeira do SENAI-SP, situada na Avenida Paulista, nº 1313, 2º andar, Bairro Bela Vista, em São Paulo – SP, em 25 (trinta) dias, fora dezena, após a entrega efetiva dos serviços e da nota fiscal respectiva, de modo que ocorram apenas nos dias 10, 20 ou 30 de cada mês.

3.4.1 Quando esses dias recaírem em finais de semana ou feriados, o pagamento será realizado no 1º dia útil subsequente.

3.5 Os pagamentos serão efetuados, em moeda corrente nacional, estando os referidos pagamentos condicionados a previsão contida na subcláusula 3.5 acima, e a aprovação dos serviços pelos SENAI-SP.

3.6 A nota fiscal deverá ser emitida no CNPJ da Escola SENAI requisitante.

3.7 Os pagamentos serão efetuados através de depósito bancário. Para tanto, deverão ser encaminhados, obrigatoriamente, as duplicatas e/ou recibos devidamente quitados.

3.8 Não deverão ser emitidos boletos bancários, bem como, não é permitido negociar os títulos.

3.9 Na hipótese de ser apresentada a documentação de cobrança com erro ou incompleta ou se concretizando circunstância que impeça a liquidação das despesas, o pagamento será suspenso e o prazo de vencimento prorrogado, se necessário até que seja providenciada as medidas saneadoras cabíveis, não acarretando, neste caso, quaisquer ônus para o SENAI-SP.

3.10 Caso a documentação para pagamento não seja entregue conforme previsto acima, o SENAI-SP poderá postergar o pagamento ficando estabelecido o vencimento da nota fiscal/fatura somente nos dias 10, 20 ou 30 do mês.

3.11 Fica vedada a negociação de duplicatas com terceiros, bem como o desconto ou a promoção de cobrança através da rede bancária, bem como qualquer forma de cessão à terceiros.

3.11.1 O descumprimento do disposto no item acima. acarretará a aplicação de penalidade(s) consignadas neste instrumento.

3.12 Se da infringência no disposto no item 3.11, advier protesto da duplicata, a CONTRATADA, além da penalidade citada acima, se obriga a efetuar à suas expensas, o respectivo cancelamento, no prazo máximo de 05 (dias), contados da data da emissão do correspondente instrumento cartorário.

3.13 Por força das legislações vigentes, se for o caso, o SENAI-SP reterá do valor bruto da nota fiscal, as alíquotas pertinentes aos tributos a seguir discriminados:

a. Imposto de Renda;
b. INSS;
c. ISS (imposto sobre serviços de qualquer natureza);
d. CSLL (contribuição social sobre lucro líquido);
e. COFINS; e,
f. PIS.

3.14 Quando da emissão da nota fiscal, a CONTRATADA deverá destacar o valor das retenções dos tributos referidos na subcláusula acima (3.13).

3.14.1 No caso da CONTRATADA ser beneficiada com decisão judicial que dispense a obrigatoriedade de retenção e recolhimento na fonte de qualquer dos tributos acima relacionados, deverá providenciar Ofício Judicial ao SENAI-SP para que cumpra a decisão judicial ou, na impossibilidade de oficiar o SENAI-SP, deverá apresentar cópias autenticadas da petição inicial, da liminar, da sentença, do acórdão e outros documentos que o SENAI-SP julgar necessários, bem como, providenciar, trimestralmente, Certidão de Objeto e Pé que comprove estar a decisão ainda em vigor na data do pagamento.

3.15 O SENAI-SP se reserva, ainda, o direito de reter quaisquer importâncias referentes a outros impostos, taxas, contribuições e recolhimentos obrigatórios, incidentes sobre a prestação dos serviços ora contratados.

3.16 O SENAI-SP poderá suspender o pagamento de qualquer nota fiscal apresentada pela CONTRATADA, no todo ou em parte, nos seguintes casos:

3.16.1 Descumprimento de obrigação relacionada com os serviços contratados;
3.16.2 Não cumprimento de obrigação contratual, hipótese em que o pagamento ficará retido até que a CONTRATADA atenda à cláusula infringida;
3.16.3 Obrigações da CONTRATADA com terceiros que, eventualmente, possam prejudicar o SENAI-SP;
3.16.4 Paralisação dos serviços por culpa da CONTRATADA; e,
3.16.5 Nos casos de suspensão dos serviços decorrente de determinação de órgão governamental que impeça a sua realização, ou que os procedimentos a serem adotados para sua realização não possam ser cumpridos pelo SENAI-SP, assegurado o pagamento dos serviços executados.

Cláusula Quarta – Das Responsabilidades da CONTRATADA

4.1. A CONTRATADA obriga-se a:

4.1.1 Executar os serviços, objeto deste contrato, de acordo com as exigências e obrigações definidas no Chamamento Público – PSDA nº 895/2025, Memorial Descritivo e demais anexos.

4.1.2 Responsabilizar-se, em caráter exclusivo, pela execução dos serviços por seus empregados, prepostos, parceiros e terceiros.

4.1.3 Executar os serviços nos prazos estabelecidos no Memorial Descritivo, Anexo B, do PSDA 109/2025 e demais anexos.

4.1.4 Arcar com eventuais custos de transporte, estadia, alimentação entre outros, necessários à execução dos serviços.

4.1.5 Considerar a vistoria e aceitação dos serviços por técnicos do SENAI-SP, se for o caso.

4.1.6 Notificar por escrito ao SENAI-SP, ao gestor do Contrato, caso ocorra qualquer fato que impossibilite o cumprimento das condições e prazos estabelecidos no contrato.

4.1.7 Responsabilizar-se por todos e quaisquer danos e/ou prejuízos que venham a causar ao SENAI-SP.

4.1.8 Solucionar eventuais falhas sem ônus ao SENAI-SP.

4.1.9 Manter, durante o tempo de vigência do contrato, os documentos de habilitação exigidos no Chamamento Público PSDA 109-2025, regularidade fiscal e regularidade técnica devidamente atualizados.

4.1.10 Manter seus profissionais devidamente identificados, com uniforme e crachá, para facilitar a sua identificação, caso haja acesso às dependências do SENAI-SP, fornecendo EPI’s, se for o caso, de acordo com as normas, regulamentos e ditames legais.

4.1.11 Apresentar documentos fiscalizatórios trabalhistas, previdenciários e demais, quando for o caso, de seus empregados, ora prestadores de serviços ao SENAI-SP.

4.1.12 Responsabilizar-se pelos pagamentos de salários, cachês, alimentação, encargos fiscais, sociais, trabalhistas e previdenciários de seus funcionários, prepostos e terceiros, e ainda, por quaisquer outras obrigações assumidas perante os profissionais mencionados nas relações de integrantes apresentadas ao SENAI-SP, obrigando a saldá-las em época própria.

4.1.13 Assumir todos os encargos de possível demanda trabalhista, civil ou penal, relacionadas à prestação dos serviços.

4.1.14 Guardar sigilo dos dados a que tiver acesso ou que vierem a ser compartilhados, bem como sobre os produtos de propriedade do SENAI-SP, além daqueles processados e gerados no ambiente físico da CONTRATADA, reconhecendo serem estes de propriedade exclusiva do SENAI-SP, os quais não podem ser cedidos, copiados, reproduzidos, publicados, divulgados de nenhuma forma, nem colocados à disposição direta ou indiretamente, locados ou vendidos a terceiros.

4.1.15 Responsabilizar-se pelos danos financeiros ou de imagem causados diretamente ao SENAI-SP ou a terceiros, até o limite do contrato, decorrentes de sua culpa ou dolo quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento pela Gerência de Infraestrutura e Suprimentos do SENAI-SP.

4.1.16 Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando forem vítimas os seus técnicos no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências do SENAI-SP.

4.1.17 Responsabilizar-se pelo cumprimento das exigências legais no que respeita às jornadas das equipes de trabalho, em seus diversos horários.

4.1.18 Manter os seus profissionais informados quanto às normas disciplinares do SENAI-SP, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações.

4.1.19 Indicar um representante para gestão do contrato e definir equipe para interação com o SENAI-SP.

4.1.20 Apresentar, quando solicitado, a licença de uso ou certificação de posse de todos os softwares de sua propriedade que serão empregados na prestação dos serviços, não cabendo ao SENAI-SP quaisquer ônus decorrentes do uso indevido de softwares pela equipe técnica da Contratada.

4.1.21 Fornecer todas as licenças, autorizações, certificados e garantias necessárias à execução do objeto, observando rigorosamente os prazos e condições estabelecidos no Chamamento Público – PSDA 109-2025, no Memorial Descritivo e demais anexos que integram o presente processo. Tais licenças e garantias deverão ser compatíveis com as especificações técnicas do objeto, conforme detalhado no Memorial Descritivo já mencionado.

4.1.22 Responsabilizar-se pelo cumprimento da legislação competente por qualquer item de reparo no ambiente, não cabendo ao SENAI-SP quaisquer ônus decorrentes.

4.1.23 Não empregar menores de 18 anos em trabalho noturno, perigoso ou insalubre e nem menores de 16 anos, em qualquer trabalho, salvo na condição de aprendiz a partir dos 14 anos.

Cláusula Quinta – Demais Obrigações da CONTRATADA

Trabalhistas e Previdenciárias

5.1 A CONTRATADA deverá cumprir todas as obrigações trabalhistas e previdenciárias relativas aos profissionais designados para a prestação de serviço, observando, especialmente, as seguintes obrigações:

a) Pagar os salários e demais verbas passadas diretamente ao seu funcionário alocado a prestação de serviço;
b) Observar as obrigações previstas na convenção, acordo coletivo, acórdão normativo ou na legislação incidente aplicável à categoria profissional do empregado, inclusive no que diz respeito a pisos salariais;
c) Cumprir as obrigações trabalhistas de acordo com os valores e especificações indicados na planilha de custos e formação de preços contida na Proposta, sempre respeitados os mínimos previstos na norma coletiva aplicável;
d) Atender a legislação relativa à segurança e à medicina do trabalho, e em particular as Normas Regulamentadoras (NR) expedidas pelo Ministério do Trabalho e Emprego; e
e) Pagar antecipadamente, em parcela única mensal, os insumos referentes a vale-transporte e auxílio-alimentação (se for o caso, ora quando aplicável).

5.2 Deve ser mantido e atualizado pela CONTRATADA, bem como exibidos por meio de cópias, sempre que solicitadas pelo SENAI-SP, os registros, anotações e documentos que comprovem o cumprimento das obrigações trabalhistas e previdenciárias, tais como:

a) O contrato de trabalho, o regulamento interno da empresa, se houver, o acordo ou a convenção coletiva de trabalho, ou ainda, o acórdão normativo, se for o caso, relativos à categoria profissional do empregado;
b) O registro do empregado e Carteira de Trabalho e Previdência Social;
c) O Atestado de Saúde Ocupacional (ASO), comprovando a realização das avaliações médicas (admissional, periódica, demissional e, se for o caso, de retorno ao trabalho e de mudança de função) e exames complementares determinados pelo médico do trabalho;
d) Documentos comprobatórios do pagamento das contribuições previdenciárias dos empregados e do empregador;
e) Cartão, ficha ou livro de ponto assinado pelo empregado, ou documento comprobatório do registro eletrônico de ponto, nos quais constem as horas trabalhadas normais e extraordinárias, se for o caso;
f) Recibo de concessão de aviso de férias, a ser dado 30 (trinta) dias antes do respectivo gozo;
g) Documento comprobatório de depósito bancário na conta do trabalhador referente ao pagamento dos salários mensais e adicionais aplicáveis, férias acrescidas do terço constitucional e décimo terceiro salário (primeira e segunda parcelas);
h) Documento comprobatório de fornecimento de auxílio-alimentação;
i) Documento comprobatório do recolhimento dos valores devidos ao FGTS nas respectivas contas vinculadas do empregado;
j) Termos que cuidem da demissão ou rescisão do contrato, sua respectiva homologação e quitação de verbas rescisórias, na forma da legislação;
k) Documento comprobatório da concessão de aviso prévio pelo empregador ou pelo empregado;
l) Documento comprobatório da entrega dos documentos necessários à obtenção de seguro-desemprego pelo empregado, nas hipóteses em que o mesmo faça jus ao benefício.

5.3 Fica estabelecido que a CONTRATADA é considerada, para todos os fins e efeitos jurídicos, como único e exclusivo empregador dos profissionais alocados na prestação de serviço, sendo o responsável pelo cumprimento das obrigações trabalhistas e previdenciárias, cabendo-lhe reembolsar o SENAI-SP ou suas subsidiárias de todas as despesas que estes tiverem, inclusive custas, emolumentos e honorários advocatícios, resultantes de sua condenação judicial a honrar obrigações trabalhistas ou previdenciárias, ou ainda a pagar indenizações decorrentes das relações de trabalho.

5.4 Respeitadas todas as previsões descritas na minuta de contrato, a CONTRATADA é a única e exclusiva responsável por todos os encargos trabalhistas, inclusive decorrentes de acordos, dissídios e convenções coletivas, previdenciários, fiscais e comerciais, oriundos da execução do contrato, podendo SENAI-SP a qualquer tempo, exigirem a comprovação do cumprimento de tais encargos, inclusive, de todos os documentos arrolados nesta cláusula, como condição do pagamento do valor ajustado no contrato.

Cláusula Sexta - Das Obrigações do SENAI-SP

6.1 O SENAI-SP se obriga a:

6.1.1 Fornecer à Contratada, em tempo hábil, as informações necessárias à execução dos serviços, bem como a documentação técnica referente aos padrões adotados, se necessário.

6.1.2 Informar à Contratada as normas e procedimentos de acesso às instalações da Gerência Sênior de Tecnologia da Informação do SENAI-SP e suas eventuais alterações.

6.1.3 Designar um funcionário para gerenciar e fiscalizar o contrato.

6.1.4 Anotar em registro próprio todas as ocorrências relacionadas à execução dos serviços mencionados, determinando o que for necessário à regularização das falhas ou defeitos observados.

Cláusula Sétima – Da Denúncia e da Rescisão

7.1. Qualquer uma das partes poderá denunciar o contrato antecipadamente, desde que comunique sua intenção com no mínimo 60 (sessenta) dias de antecedência.

7.2 O presente contrato poderá ser rescindido em caso de descumprimento de quaisquer de suas cláusulas contratuais, arcando a parte que der motivo, com o pagamento à parte inocente, da multa contratual prevista neste instrumento, caso a parte inadimplente, após notificada, não adimplir com sua obrigação no prazo de 03 (três) dias corridos a partir do recebimento da notificação.

7.3 Por iniciativa motivada do SENAI-SP, o contrato ainda poderá ser reincidido:

a) pela infração a qualquer cláusula do presente contrato;
b) se a CONTRATADA paralisar o serviço pelo espaço de 10 (dez) dias consecutivos, sem motivo justificado;
c) em caso de recuperação judicial/extrajudicial, falência, dissolução ou liquidação da CONTRATADA;
d) em caso de atraso superior a 10 (dez) dias no cumprimento de qualquer etapa do cronograma físico, ou lentidão na execução dos serviços de que resulte, comprovadamente, a impossibilidade de sua conclusão no prazo estipulado;
e) se o SENAI-SP achar por bem paralisar a qualquer título, adiar ou cancelar a obra, por sua única e exclusiva conveniência.
f) na hipótese de suspensão dos serviços por determinação de autoridades competentes, ficando a CONTRATADA responsável pelos eventuais aumentos nos custos de serviços e pelas perdas e danos que o SENAI-SP venha a sofrer;
g) decorrente de associação com outrem, fusão ou incorporação da CONTRATADA, ou ainda alteração de seu Contrato Social ou Estatuto, que modifique seu objeto, estrutura ou prejudique a execução deste contrato;
h) pela subcontratação total, cessão ou transferência do contrato;
i) em caso de subcontratação parcial dos serviços, sem prévia concordância do SENAI-SP; e,
j) cometimento reiterado de faltas ou não atendimento das determinações da fiscalização do SENAI-SP.

Cláusula Oitava – Da Confidencialidade

8.1 A CONTRATADA deverá assinar o termo de confidencialidade do SENAI-SP, de forma a respeitar a confidencialidade, integridade e disponibilidade das informações relacionadas a prestação de serviços em questão, sob pena de multa e rescisão contratual.

8.2 As partes deverão manter completo e absoluto sigilo sobre quaisquer dados, materiais, informações, documentos, especificações técnicas e inovações que tenha acesso umas das outras, em virtude da prestação dos serviços objeto deste contrato, não podendo sob qualquer pretexto divulgar, revelar, reproduzir, utilizar ou dar conhecimento a terceiros, sob pena de rescisão deste instrumento e, ainda,

de serem obrigadas a responderem, eventualmente, pela responsabilidade civil e penal advinda da divulgação de informações sigilosas. A obrigação de confidencialidade deverá ser cumprida do início da vigência deste contrato até 05 (cinco) anos após o término da vigência ou da denúncia ou rescisão deste ajuste.

8.3. De igual forma, as partes concordam, salvo quando exigido por lei ou por ordem judicial, a não disponibilizar as informações confidenciais da outra parte, por qualquer meio, a terceiros, para qualquer finalidade, exceto para a implementação do presente contrato e observadas as demais disposições deste contrato e demais instrumentos que o integram.

8.4. As partes concordam e obrigam-se a providenciar todas as medidas para assegurarem que as informações confidenciais não sejam divulgadas ou distribuídas por seus empregados ou agentes, em violação aos dispositivos do presente instrumento, restringindo, obrigatoriamente, o acesso às citadas informações apenas daqueles funcionários designados para a consecução do objeto deste contrato.

8.5. A informação confidencial de uma das partes não inclui informação que:

a) Seja ou se torne, no decorrer do prazo contratual, parte do domínio público, independente de ação ou omissão da outra parte;

b) Embora de conhecimento legítimo da outra parte, anteriormente à revelação, não tenha sido obtida diretamente ou indiretamente da parte reveladora;

c) Legitimamente revelada à outra parte por uma terceira pessoa sem restrição sobre a revelação; e,

d) Seja independente desenvolvida pela outra parte.

Cláusula Nona – Das Condições Gerais

9.1 A CONTRATADA é a única e exclusiva responsável por quaisquer danos ou prejuízos, que eventualmente possa causar a terceiros, bem como seus prepostos e empregados, em decorrência da execução dos serviços objeto do presente ajuste, sem que possa ser imputada qualquer responsabilidade ou ônus ao SENAI-SP pelos ressarcimentos ou indenizações devidos.

9.2 Na hipótese do SENAI-SP, por meio da Gerência de Infraestrutura e Suprimentos do SENAI-SP, vir a exigir a comprovação do cumprimento de todas as obrigações legais a que se sujeita a CONTRATADA, tal comprovação deverá ser realizada mediante a apresentação dos documentos, demonstrando que se encontra em dia com todos os recolhimentos, conforme for o caso, dos tributos, contribuições, taxas, encargos trabalhistas e previdenciários, e de demais documentos legais que o SENAI-SP, a seu exclusivo critério, entendam ser necessários.

9.3 O SENAI-SP não será responsável, seja a que título for, por quaisquer perdas, danos, extravios ou desaparecimento de objetos pertencentes à CONTRATADA ou aos membros da sua equipe.

9.4 Caso a CONTRATADA não apresente ou apresente a documentação incompleta solicitada pelo SENAI-SP, tal fato ensejará a imediata suspensão do pagamento de qualquer valor, que somente será efetuado mediante a regularização da falta, sem prejuízo do presente instrumento ser rescindido pelo SENAI-SP por inadimplemento contratual por parte da CONTRATADA, com pagamento da multa contratual aqui estipulada e apuração de perdas e danos.

9.5 Fica estabelecido que o SENAI-SP não responderá, sob qualquer hipótese, pelos ônus decorrentes do uso indevido de equipamentos, programas de computador e demais ferramentas e recursos auxiliares protegidos nos termos da lei, que a CONTRATADA tenha violado na execução dos serviços objeto deste instrumento, cabendo à mesma CONTRATADA responder, civil e penalmente, por eventuais infrações cometidas.

9.6 Na assinatura do contrato a CONTRATADA toma ciência da Política de Segurança de Informação do SENAI-SP firmando o documento Termo de Confidencialidade, conforme destacado na cláusula décima, cujo conteúdo deverá ser divulgado a todos os seus profissionais que integrarão a equipe de prestação de serviços do SENAI-SP, de maneira que os termos ali consignados sejam efetivamente conhecidos e adotados.

9.7 Qualquer tolerância no cumprimento do presente instrumento será entendida como mera liberalidade das partes e não como novação, que não se presumirá em nenhuma hipótese, configurando-se apenas por escrito e firmada por ambas as Partes.

9.8 As Partes cumprirão integralmente, a todo tempo, de acordo com a Lei Anticorrupção Brasileira (Lei nº 12.846/2013), bem como com todas as outras leis antissuborno, anticorrupção, sobre conflitos de interesse ou outras leis, normas ou regulamentos com finalidade e efeito semelhantes aplicáveis à CONTRATADA ou ao SENAI-SP.

9.9 Se durante a vigência do presente contrato, o SENAI-SP for obrigado, por Lei ou Ato de Autoridade Pública, a interromper as atividades que constituem o objeto deste contrato, o mesmo poderá ser (extinto) rescindido, independente do pagamento da multa ou qualquer outra verba, seja a que título for.

9.10 Se durante a vigência do presente contrato ocorrer motivos de caso fortuito e/ou de força maior que impeça a continuidade da execução do contrato, tais como calamidades públicas, estado de emergência, que gerem impacto de forma a restringir circulação de pessoas por medida de segurança pública, motivos de interesse público e/ou bem estar social, declarado/s ou não por Autoridade/s, Comunicado/s emitido/s pela Organização Mundial da Saúde ou Organismos Governamentais, poderá ocorrer a suspensão do presente instrumento, e se for o caso, com o cancelamento de cronogramas definidos, até o seu regular retorno, sem que haja qualquer penalidade, custo e despesa, a quaisquer das Partes, seja a que título for.

9.11 Na eventualidade de vir a ser exigida do SENAI-SP qualquer importância de responsabilidade da CONTRATADA, esta ficará obrigada a repor ao SENAI-SP o valor por ele despendido, acrescido de 50% (cinquenta por cento).

9.12 Fica estabelecido que a CONTRATADA é considerada, para todos os fins e efeitos jurídicos, como único e exclusivo empregador dos profissionais alocados na prestação de serviço, sendo o responsável pelo cumprimento das obrigações trabalhistas e previdenciárias, cabendo-lhe reembolsar o SENAI-SP ou suas subsidiárias de todas as despesas que estes tiverem, inclusive custas, emolumentos e honorários advocatícios, resultantes de sua condenação judicial a honrar obrigações trabalhistas ou previdenciárias, ou ainda a pagar indenizações decorrentes das relações de trabalho

Cláusula Décima – Gestão e Fiscalização

Os serviços inerentes ao presente contrato serão conduzidos sob a fiscalização da Gerência de Infraestrutura

e Suprimentos do SENAI-SP, que indicará funcionário(s) que exercerá(ão) a função de gestor(es) de contrato, responsável(is) por acompanhar a execução, as etapas e prazos determinados, conferir os documentos e relatórios (se for o caso), atestar a realização dos serviços para liberação dos pagamentos correspondentes.

Cláusula Décima Primeira – Da Lei Geral de Proteção de Dados

11.1. As Partes declaram que cumprirão a Lei Geral de Proteção de Dados ("LGPD") nº 13.709, de 14 de agosto de 2018 e todas as demais leis, normas e regulamentos aplicáveis, assim como cumprirão suas respectivas atualizações e atenderão os padrões aplicáveis em seu segmento em relação ao tratamento de dados pessoais, tanto no que diz respeito aos dados pessoais disponibilizados pelo SENAI-SP à CONTRATADA, quanto com relação aos dados disponibilizados pela CONTRATADA ao SENAI-SP, pelo que se segue:

a) Possuem todos os direitos, consentimentos e/ou autorizações necessários exigidos pela LGPD, e demais leis aplicáveis, para divulgar, compartilhar e/ou autorizar o tratamento dos dados pessoais para o cumprimento de suas obrigações contratuais e/ou legais;
b) Não conservarão dados pessoais que excedam as finalidades previstas no Contrato e seus anexos;
c) Informarão e instruirão os seus colaboradores, prestadores de serviços e/ou terceiros sobre o tratamento dos dados pessoais, observando todas as condições desse Contrato, inclusive na hipótese de os titulares de dados terem acesso direto a qualquer sistema (on-line ou não) para preenchimento de informações que possam conter os dados pessoais, garantindo a privacidade e confidencialidade dos dados pessoais, e mantendo um controle rigoroso sobre o acesso aos dados pessoais;
d) Não fornecerão ou compartilharão, em qualquer hipótese, dados pessoais sensíveis de seus colaboradores, prestadores de serviços e/ou terceiros, salvo se expressamente solicitado por uma Parte à outra, caso o objeto do Contrato justifique o recebimento de tais dados pessoais sensíveis, estritamente para fins de atendimento de legislação aplicável;
e) Informarão uma Parte à outra sobre qualquer incidente de segurança, relacionado ao presente instrumento, em até 48 (quarenta e oito) horas, contadas do momento em que tomou conhecimento, por quaisquer meios, do respectivo incidente;
f) Irão alterar, corrigir, apagar, dar acesso, anonimizar ou realizar a portabilidade para terceiros de dados pessoais mediante solicitação da Parte requerente e garantirá que todos os dados pessoais que forem objeto de tratamento sejam precisos e atualizados;
g) Excluirão, de forma irreversível, os dados pessoais retidos em seus registros, mediante solicitação da outra Parte ou dos titulares dos dados, a qualquer momento, salvo conforme determinado por lei ou ordem judicial;
h) Implementarão medidas de segurança substancialmente, quando for o caso, de acordo com os padrões aplicáveis na indústria projetados para garantir a segurança, confidencialidade e integridade dos Dados Pessoais;
i) Colaborarão com a outra PARTE, mediante solicitação desta, no cumprimento das obrigações de responder a solicitações e reivindicações de pessoa e/ou autoridade governamental, a respeito de Dados Pessoais;
j) Ao término do Contrato cessará o tratamento, inclusive qualquer uso dos Dados Pessoais e devolverá à outra PARTE ou destruirá todos os Dados Pessoais e todas as cópias destes, exceto se obrigada a manter cópia de determinados Dados Pessoais estritamente em virtude de lei;
k) O tratamento dos dados coletados, somente quando autorizados, de uma Parte à outra, poderão ser conservados pelo período de 5 (cinco) anos após o término do presente instrumento, com sua posterior eliminação, sendo autorizada sua conservação nas hipóteses descritas no artigo 16 da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018)
l) Assegurarão que colaboradores, prestadores de serviços, terceiros, parceiros e membros da equipe técnica que venham ter acesso aos dados durante o desenvolvimento do projeto cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais, nunca cedendo ou divulgando

tais dados a terceiros, salvo se expressamente autorizado pelo titular, por força de lei ou determinação judicial;

m) As PARTES não poderão subcontratar nem delegar o Tratamento dos Dados Pessoais sem o consentimento prévio por escrito da outra PARTE, mas podem as PARTES preservar e conservar os dados por si ou por empresa CONTRATADA especialmente para este fim;

n) As PARTES declaram ciência de que os dados fornecidos, uma vez anonimizados, não são considerados DADOS PESSOAIS, como estabelece o artigo 12 da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).

11.2. Independentemente do disposto em qualquer outra cláusula deste Contrato, ou se for o caso do Contrato original e eventuais aditivos, a CONTRATADA é a única responsável por todo e qualquer dano decorrente do descumprimento da LEI Nº 13.709, de 14 de agosto de 2018 – Lei de Proteção dos Dados, pela CONTRATADA, por seus colaboradores, prepostos, subcontratados, parceiros comerciais, empresas afiliadas ou qualquer agente ou terceiro a ela vinculado ou que atue em seu nome.

Cláusula Décima Segunda – Da Garantia

12.1 Os serviços executados no escopo da presente contratação terão garantia irrestrita durante a vigência integral do contrato, inclusive para os períodos de prorrogações.

12.2 Poderá solicitar, dentro do período de garantia, sem qualquer ônus adicional, a correção ou nova execução de serviços, produtos ou documentos entregues que apresentem problemas ou necessidade de correções.

12.3 Deverá assegurar garantia durante 12 meses para todos os itens do software fornecido, inclusive para os períodos de eventuais prorrogações do contrato.

12.4 A garantia inclui as atualizações de softwares fornecidos e portabilidade de softwares, ambos dentro dos prazos vigentes do contrato, sem ônus financeiro adicional.

Cláusula Décima Terceira – Das Penalidades

13.1 Atrasos ou descumprimento de quaisquer das cláusulas estabelecidas neste contrato ou a sua reincidência, acarretará a aplicação de multa no percentual de 2% (dois por cento) do valor total do contrato, sem prejuízo do direito da parte prejudicada de exigir eventual indenização por perdas e danos.

13.2 A parte que der motivo à rescisão, por atrasos, descumprimentos das cláusulas e condições constantes deste ajuste, incorrerá no pagamento, à parte inocente da multa contratual equivalente a 10% (dez por cento) do valor total do contrato, ressalvado o direito ao credor de exigir indenização por prejuízo excedente, nos termos do parágrafo único do art. 416 do Código Civil.

13.3 O inadimplemento total ou parcial das obrigações contratuais assumidas pela CONTRATADA, dará ao SENAI-SP o direito de rescindir unilateralmente o contrato, sem prejuízo de outras penalidades previstas neste ajuste, inclusive a de suspensão do direito de participar de procedimento licitatório junto ao SESI-SP e ao SENAI-SP por prazo não superior a 05 (cinco) anos, impedimento esse extensivo às pessoas físicas que constituíram a pessoa jurídica, as quais permanecem impedidas de licitar enquanto perdurarem as causas da penalidade, independentemente de nova pessoa jurídica que vierem a constituir ou de outra em que figurem como sócios, e às pessoas jurídicas que tenham sócios comuns com as pessoas físicas acima mencionadas.

13.4 As penalidades aqui previstas são independentes, não excludentes e poderão ser aplicadas

cumulativamente, quando for o caso.

13.5 Os valores relativos as multas aplicadas, bem como, outros valores que forem devidos serão deduzidos dos créditos que a contratada possuir com o SENAI-SP ou cobrados administrativa ou judicialmente.

Cláusula Décima Quarta – Da Assinatura Eletrônica

14.1 Quando for o caso, como alternativa à assinatura física, as Partes declaram e concordam que a assinatura deste Instrumento e todos os seus aditivos e afins poderá ser realizada eletronicamente.

14.2 As Partes reconhecem a veracidade, autenticidade, integridade, validade e eficácia deste Instrumento, de acordo com o art. 219 do Código Civil, em formato eletrônico e assinado pelas Partes por meio de certificados eletrônicos, nos termos do art. 10, da Medida Provisória nº 2.220-2, de 24 de agosto de 2001 ("MP 2.220-2"), declarando, desde já, plena anuência com a aposição das assinaturas eletrônicas neste Contrato na plataforma a ser definida pelas Partes.

14.3 Adicionalmente, as Partes signatárias deste Instrumento expressamente anuem, autorizam, aceitam e reconhecem como válida qualquer forma de comprovação da autoria de suas respectivas assinaturas por meio de certificados eletrônicos, nos termos da MP 2.220-2, de 24/08/2001, sendo certo que quaisquer de tais certificados será suficiente para comprovar a veracidade, autenticidade, integridade, validade e eficácia deste Contrato e seus termos, bem como a respectiva vinculação das Partes às suas disposições, nos termos dos artigos 441 e 784, III, do Código de Processo Civil.

Cláusula Décima Quinta – Da Representação da CONTRATADA

A CONTRATADA declara neste ato, para todos os fins e efeitos de direito, que o(s) signatário(s) é(são) seu(s) legítimo(s) representante(s) na data de assinatura deste instrumento, conforme documentos societários e quando for o caso, procuração, constantes de seu cadastro junto ao SENAI-SP, estando ciente de que a falsidade na prestação desta informação, sem prejuízo de serem aplicadas as penalidades previstas neste instrumento, inclusive sua rescisão e apuração de perdas e danos, sujeitará todas as pessoas que para ela concorrem, às penalidades previstas na legislação criminal relativas à falsidade ideológica (art. 299 do Código Penal).

Cláusula Décima Sexta – Do Foro

O Foro para qualquer postulação decorrente do presente Contrato é o da cidade de São Paulo, excluindo-se qualquer outro por mais privilegiado que seja ou venha a se tornar.

Assim, justas e contratadas, as partes assinam o presente em 2 (duas) vias, para um só efeito, na presença das testemunhas abaixo identificadas.

São Paulo, de de 20 .

SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI
Departamento Regional de São Paulo

_____

Nome:

Diretor da Escola SENAI Paulo Antônio Skaf

_____

CONTRATADA

_____

(Repres. Legal)

Nome(s):

CPF(s):

Cargo(s):

Testemunhas:

_____ _____

Nome: Nome:

RG n.º RG n.º

ANEXO E

TERMO DE CONFIDENCIALIDADE

Pelo presente instrumento particular, e na melhor forma de direito, em que são partes contratantes, de um lado, o SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI, Departamento Regional de São Paulo, inscrito no CNPJ sob o n.º 03.774.819/0001-02, com sede na Avenida Paulista, nº 1313, 3º andar, Bairro da Bela Vista, na Cidade de São Paulo, Estado de São Paulo, neste ato representado por _____, Gerente _____, doravante, denominado, simplesmente, SENAI-SP, e, de outro lado, a empresa _____, inscrita no CNPJ/MF sob o nº _____, com sede na _____, n.º _____ – Bairro_____ CEP _____, na cidade de _____, Estado de _____, aqui representada em conformidade com seus atos constitutivos, resolvem formalizar o presente termo, considerando que:

a segurança e/ou proteção da informação é aqui caracterizada pela preservação da: **CONFIDENCIALIDADE** (garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso), **INTEGRIDADE** (salvaguarda da exatidão e completeza da informação e dos métodos de processamento), e **DISPONIBILIDADE** (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e,

(a) o **SENAI-SP** e a empresa resolvem firmar o presente instrumento, doravante denominado de "TERMO DE CONFIDENCIALIDADE", que se regerá pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA: DAS INFORMAÇÕES CONFIDENCIAIS

1.1 São consideradas informações confidenciais, portanto, protegidas pelo presente termo, todos os dados de natureza técnica, operacional, comercial, jurídica e financeira, bem como toda e qualquer informação que venha a ser "trocada" entre as partes, salvo aquelas cuja confidencialidade seja expressamente afastada.

1.2 A forma através da qual suceder a troca ou o acesso às informações classificadas é irrelevante para os efeitos deste acordo, sendo que os documentos impressos, manuscritos, *fac-símiles*, *laser-discs*, *pendrives*, disquetes ou qualquer outro meio onde estejam armazenados dados confidenciais, devem ser mantidos em local seguro (com acesso restrito) e destruídos ou devolvidos à proprietária da informação, após sua devida utilização, conforme orientação fornecida por esta última.

CLÁUSULA SEGUNDA: DAS OBRIGAÇÕES DA RECEPTORA

2.1 A empresa compromete-se por todos aqueles que por seu intermédio venham a tomar conhecimento de informações confidenciais do **SENAI-SP**, a manter o mais absoluto sigilo, limitando a utilização dos dados disponibilizados às estritas necessidades da negociação, contrato ou similar, não utilizando, em hipótese alguma, tais informações em proveito próprio ou alheio.

2.2 Fica a empresa expressamente proibida de transferir a terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações classificadas a que tenha tido acesso, no território brasileiro ou no exterior, para nenhuma pessoa física ou jurídica e para nenhuma outra finalidade que não seja a consecução de seus objetivos conjuntos com o SENAI-SP.

2.3 Obriga-se a empresa a adotar todas as cautelas possíveis, no sentido de restringir o acesso às informações

confidenciais em seu poder e impedir sua indevida divulgação ou utilização, valendo-se de ações destinadas a evitar o “vazamento” das informações classificadas.

2.4 As informações confidenciais que venham a ser confiadas à empresa somente poderão ser repassadas aos administradores, prepostos e terceiros diretamente envolvidos no processo e cujo acesso seja indispensável para consecução da transação, negociação ou contratação em curso, sendo estes advertidos do caráter sigiloso das informações, e ficando a empresa expressamente responsável em caso de quebra na integridade e sigilo destes dados.

2.5 É vedado à empresa, em qualquer hipótese, manter em seu poder após sua utilização, documento ou qualquer outro meio onde as informações confidenciais do **SENAI-SP** estejam consignadas, ficando expressamente proibida a extração de cópias, reproduções, *backup* ou outro meio de armazenamento de dados.

2.6 A empresa compromete-se a contatar a proprietária da informação confidencial, caso eventualmente perceba a necessidade de repassar a terceiros, informação classificada, ainda que o repasse seja de apenas parte da informação, oportunidade em que deverá ser firmado, se for do interesse da proprietária, outro termo de confidencialidade obrigando a totalidade das partes.

2.7 A empresa deverá comunicar o extravio, perda ou violação de qualquer informação confidencial, não ficando responsável nem sendo considerada violação ao presente acordo no caso da informação confidencial ser divulgada em razão de ato ou fato ao qual a empresa ou qualquer de seus empregados, prepostos e/ou colaboradores que for divulgada em decorrência de fatos que tenham ocorrido em razão de caso fortuito e/ou força maior.

2.8 Se por decisão judicial a empresa for obrigada a revelar informação ou dado que venha, ainda que indiretamente, a expor informação confidencial do **SENAI-SP**, este deverá ser previamente comunicado.

2.9 Não serão consideradas informações confidenciais aquelas que sejam do prévio conhecimento da empresa, de conhecimento público ou que venham a se tornar públicas por expressa vontade da proprietária da informação.

CLÁUSULA TERCEIRA: DAS INFORMAÇÕES CONJUGADAS

Na hipótese de surgirem informações relevantes da própria relação entre as partes, ou seja, se as informações confidenciais do **SENAI-SP** forem conjugadas com outros dados confidenciais da empresa / pessoa física, estas serão consideradas informações classificadas de propriedade conjunta do **SENAI-SP**, sendo que sua divulgação e utilização somente sucederão mediante prévia e expressa autorização de ambas as partes.

CLÁUSULA QUARTA: DA UTILIZAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

4.1. Nos precisos termos da cláusula primeira, o presente termo tem por objeto principal possibilitar à empresa o acesso a informações confidenciais do **SENAI-SP**, indispensáveis para a realização de negociação ou transação comercial, sem importar, contudo, em qualquer transferência ou cessão de informações.

4.2. As informações confidenciais são utilizáveis única e exclusivamente por seu proprietário, não autorizando o presente instrumento, seu uso pela empresa, a não ser para a fiel execução de negociação, contrato ou qualquer outra transação que envolva o proprietário da informação.

4.3. Os direitos resultantes das informações confidenciais ou de seu emprego, bem como qualquer outro direito relativo à propriedade dessas informações também não se transferem através do presente.

CLÁUSULA QUINTA: DAS DISPOSIÇÔES GERAIS

5.1 Os empregados/prepostos da empresa se comprometem a conhecer, observar e agir em conformidade com as Políticas de Segurança da Informação do **SENAI-SP** e/ou outras diretrizes, normas, instruções de trabalho e procedimentos relacionados, protegendo e preservando a integridade e confidencialidade de todos os dados e informações dos quais tome conhecimento ou utilize no exercício das suas funções, que serão tidos como sigilo profissional, inclusive após a cessação das suas atividades no **SENAI-SP**; estando cientes de que o desrespeito às diretrizes, normas e procedimentos relacionados com a segurança da informação e outras normas e procedimentos do **SENAI-SP** de que tenha sido dado conhecimento durante o exercício das suas funções, constitui *Violação de Segurança da Informação* e que, em caso de desrespeita-las, ficarão sujeitos às sanções previstas em lei e normas externas.

5.2 A existência e o conteúdo desse **Termo de Confidencialidade**, bem como a execução das atividades dos empregados da empresa a serviço do **SENAI-SP** não poderão ser reveladas a terceiros.

5.3 A seleção das informações confidenciais, a serem disponibilizadas para os empregados da empresa será de exclusivo critério do **SENAI-SP**.

5.4 Fica expressamente entendido que ao revelar as informações confidenciais para a empresa, o **SENAI-SP** não estará concedendo qualquer tipo de licença, expressa ou implícita, nem transferindo direitos de qualquer espécie sobre tais informações.

5.5. As partes, no âmbito das relações de trabalho que mantem com seus empregados e/ou prepostos, e nos limites e na proporção de suas responsabilidades, inclusive as de natureza tributária, responderão por todas as obrigações sociais, fiscais, parafiscais, trabalhistas, inclusive de previsão em normas coletivas das categorias, previdenciárias e sanitárias, que incidam ou venham a incidir sobre este Termo e; sobre os serviços eventualmente contratados, com terceiros, aí incluídas as relativas a acidentes de trabalho. Responderão, também, nas esferas civil e trabalhista pelos atos praticados por seus empregados e prepostos, quando da execução das atividades objeto deste Termo, suportando os ônus decorrentes de quaisquer danos, materiais e/ou morais, que os mesmos venham a causar aos bens e às pessoas.

CLÁUSULA SEXTA: DA DURAÇÃO

6.1 O acordo vigorará pelo período de 12 meses contados da data de sua assinatura, ou até o término do contrato que porventura venha a ser celebrado entre as partes, relacionado com o propósito deste acordo, podendo ser terminado, a qualquer tempo durante a sua vigência, por mútuo acordo entre as partes ou após notificação por escrito de uma parte à outra.

6.2 O término do acordo não desobriga as partes quanto às obrigações de confidencialidade aqui estipuladas anteriormente à efetiva data de seu encerramento, devendo a EMPRESA manter sigilo sobre as informações confidenciais recebidos por 5 (cinco) anos após sua recepção.

CLÁUSULA SÉTIMA: DAS PENALIDADES

7.1 A inobservância do dever de confidencialidade ora firmado e de qualquer das disposições deste instrumento é motivo relevante para o encerramento de toda e qualquer relação negocial existente entre as

partes e a parte culpada será obrigada a ressarcir perdas e danos que venham a ocorrer à outra parte.

7.2 A empresa será considerada infratora nos termos da legislação civil e criminal, na hipótese em que o sigilo da informação seja violado por qualquer pessoa a ela vinculada ou que tenha, por seu intermédio, obtido acesso às informações, exceto nos casos de caso fortuito e/ou força maior, se assim apurado.

CLÁUSULA OITAVA: DA REPRESENTAÇÃO DAS PARTES

As partes declaram neste ato, para todos os fins e efeitos de direito, que o(s) signatário(s) é(são) seu(s) legítimo(s) representante(s) na data de assinatura deste instrumento, estando cientes de que a falsidade na prestação desta informação, sem prejuízo de serem aplicadas as penalidades previstas neste instrumento, inclusive sua rescisão e apuração de perdas e danos, sujeitará todas as pessoas que para ela concorrem, às penalidades previstas na legislação criminal relativas à falsidade ideológica (art. 299 do Código Penal).

CLÁUSULA NONA: DO FORO

Fica eleito o foro da cidade de São Paulo, Capital, para dirimir dúvidas, controvérsias, ou desentendimentos que porventura ocorram entre as partes, a respeito do presente Termo de Confidencialidade, com exclusão de qualquer outro, por mais privilegiado que seja.

E por estarem assim justas e convencionadas, assinam as partes o presente Termo de Confidencialidade em 02 (duas) vias de igual teor e para um só efeito, na presença das testemunhas abaixo identificadas.

São Paulo, ___ de _____ de 202__.

CONTRATANTE
SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI
Departamento Regional de São Paulo

_____
..._____
Gerente _____

CONTRATADA
EMPRESA_____

_____
Representante Legal
Nome: _____
Cargo: _____

CPF: _____

Testemunhas:

_____ _____

Nome: _____ Nome: _____

RG n.º _____ RG n.º _____