ANEXO - CONTRATO DE FORNECIMENTO / EXECUÇÃO DE SERVIÇOS

CONTRATO DE FORNECIMENTO DE BENS E/OU SERVIÇOS 0030/2025 REFERENTE AO PROCESSO ADMINISTRATIVO 0084/2025, QUE ENTRE SI FIRMAM O SERVIÇO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS DO ESTADO DE SÃO PAULO – SEBRAE-SP E A EMPRESA LAYER TECNOLOGIA DA INFORMAÇÃO LTDA.

QUADRO INFORMATIVO DO INSTRUMENTO CONTRATUAL

1. OBJETO: Registro de Preços para contratação de empresa para o fornecimento de Solução de Geren-ciamento de Exposição Contínua a Ameaças Cibernéticas, com serviços de implantação, suporte técnico e repasse de conhecimento, para atendimento as demandas do SEBRAE-SP.

2. VIGÊNCIA: 24 (vinte e quatro) meses, contados da data da conclusão das assinaturas dos representantes legais das partes, podendo ser prorrogada, a critério do SEBRAE-SP, conforme disposições do Regulamento de Licitações e de Contratos do Sistema SEBRAE.

3. VALOR TOTAL DO CONTRATO: R$ 2.309.500,00 (Dois milhões, trezentos e nove mil e quinhentos reais)

DAS PARTES E SEUS REPRESENTANTES

CONTRATANTE: SERVIÇO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS DO ESTADO DE SÃO PAULO – SEBRAE-SP, com sede na Rua Vergueiro, 1.117, Paraíso, CEP: 01.504-001, São Paulo/SP, devidamente inscrito no CNPJ sob o nº 43.728.245/0001-42, neste ato representado por neste ato representado por seu Diretor de Administração e Finanças, REINALDO PEDRO CORREA, e pelo gerente da Unidade Tecnologia Corporativa, CARLOS KAZUNARI TAKAHASHI.

OFERTANTE: LAYER TECNOLOGIA DA INFORMAÇÃO LTDA, sociedade empresária com sede na SHN, Quadra 1, Conjunto A, Bloco A, Entrada A, S/N, Salas 708/709, Edifício Le Quartier, Asa Norte, Brasilia/DF, CEP: 70.701-010, inscrita no CNPJ sob o nº 04.929.322/0001-70, neste ato representada por seus sócios, RODRIGO GARCIA MEDEIROS e VICTOR ARAUJO FREIRE.

DO FUNDAMENTO LEGAL

A presente contratação é proveniente do Pregão Eletrônico SRP nº **90051/2025,** referente ao processo **0084/2025**, o qual resultou na Ata de Regitro de Preço nº **0024/2025**.

CLÁUSULAS CONTRATUAIS

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Por meio do presente instrumento, a CONTRATADA se obriga a fornecer ao CONTRATANTE os bens e/ou serviços especificados na proposta comercial, proveniente da Ata de Registro de Preços nº **0024/2025**, os quais, independentemente de transcrição, são partes integrantes deste instrumento e serão observados naquilo que não o contrarie.

2. CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DAS PARTES

2.1. São obrigações da CONTRATADA, sem prejuízo de outras previstas neste instrumento e respectivos anexos:

2.1.1. Entregar o objeto do contrato previsto na cláusula primeira dentro dos prazos, quantidades, características, detalhamentos e níveis estabelecidos;

2.1.2. Prestar garantia e assistência técnica conforme disposto no Termo de Referência e no Termo de Garantia Técnica, se for o caso;

2.1.3. Cumprir todas as leis e imposições federais, estaduais e municipais pertinentes;

2.1.4. Responsabilizar-se por todos os prejuízos decorrentes de infrações a que houver dado causa, pela ação ou omissão total ou parcial, inclusive por quaisquer ações judiciais relacionadas com o cumprimento do presente contrato;

2.1.5. Efetuar o pagamento de todos os tributos, seguros, obrigações sociais, trabalhistas, previdenciárias, societárias ou outras, incidentes ou que vierem a incidir sobre o objeto do contrato, até o seu recebimento, bem assim quaisquer despesas diretas e/ou indiretas relacionadas com a execução deste contrato, comprovando, a qualquer momento, os respectivos pagamentos que incidirem sobre a execução.

2.1.6. Apresentar as Notas Fiscais/Faturas contendo a discriminação exata e os respectivos quantitativos, com os valores contratados;

2.1.7. Manter, durante toda a execução do Contrato, as condições de habilitação e qualificação exigidas para a contratação;

2.1.8. Manter sigilo, sob pena de responsabilidade, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução contratual, devendo orientar seus empregados nesse sentido;

2.1.9. Prestar informações e esclarecimentos sobre eventuais atos ou fatos noticiados que envolvam a CONTRATADA, independentemente de solicitação, e atender às solicitações e determinações do CONTRATANTE.

2.1.10. Apresentar cópia das alterações estatutárias;

2.1.11. Designar formalmente profissional que seja responsável pelo relacionamento estratégico com o CONTRATANTE, com autonomia para tomada de decisões que impactem no bom andamento dos serviços, informando no prazo de até 05 (cinco) dias úteis da assinatura do contrato o e-mail, telefone fixo e móvel e nome do respectivo responsável, mantendo ativos e operacionais os meios de comunicação pelos quais serão realizadas as interações entre o CONTRATANTE e a CONTRATADA.

2.1.12. Entregar ao gestor do Contrato o Termo de Recebimento Provisório, se exigível;

2.1.13. Disponibilizar e fornecer todas as condições necessárias para o CONTRATANTE supervisionar, fiscalizar, avaliar e auditar o cumprimento do objeto deste contrato, sob os aspectos técnico, administrativo e financeiro;

2.1.14. Providenciar as exigências previstas neste instrumento e demais documentos integrantes deste contrato, respeitando os prazos previstos, sendo certo que este prazo não se confunde com a execução do contrato;

2.1.15. Registrar em relatórios de atendimento todas as reuniões de serviço entre o CONTRATANTE e a CONTRATADA, devendo ser enviados ao CONTRATANTE até o prazo máximo de 02 (dois) dias úteis após a realização do

contato e/ou reunião, podendo o CONTRATANTE solicitar a necessária correção, no prazo máximo de 02 (dois) dias úteis, a contar da data do recebimento do respectivo relatório;

2.1.16. Solucionar todos os eventuais problemas pertinentes ou relacionados com a execução do objeto deste contrato, mesmo que para isso outra solução não prevista tenha que ser apresentada para aprovação e implementação, sem ônus adicionais para o CONTRATANTE;

2.1.17. Não caucionar ou utilizar este contrato em qualquer operação financeira, salvo com anuência do CONTRATANTE;

2.1.18. Não utilizar a marca SEBRAE ou qualquer material desenvolvido pelo CONTRATANTE, salvo quando necessário a execução do objeto contratual, mediante autorização prévia;

2.1.19. Administrar e executar todos os contratos firmados com terceiros, bem como responder por todos os efeitos desses contratos perante terceiros e o próprio CONTRATANTE;

2.1.20. Cumprir a legislação trabalhista e previdenciária com relação a seus funcionários, e, quando for o caso, com relação a funcionários de terceiros contratados;

2.1.21. Reparar prontamente os danos ou avarias causadas por seus funcionários ou terceiros, aos bens do CONTRATANTE ou de terceiros, podendo o CONTRATANTE exercer o direito de retenção sobre o pagamento devido à CONTRATADA para garantia do ressarcimento do dano, total ou parcial;

2.1.22. Caso o Termo de Referência expressamente autorize a subcontratação, esta não poderá abranger a totalidade dos serviços objeto deste contrato, sendo admitida apenas em relação a serviços específicos e às expensas e riscos da CONTRATADA. Os limites da subcontratação serão estabelecidos no Termo de Referência, e sua formalização estará condicionada à prévia e expressa autorização escrita do CONTRATANTE, inclusive para substituição de qualquer subcontratação. A subcontratação não isentará a CONTRATADA de suas obrigações e responsabilidades assumidas neste CONTRATO, permanecendo íntegra e inalterada a responsabilidade da CONTRATADA pelo integral cumprimento de todos os serviços, como se diretamente os tivesse executado, não podendo opor ou transferir para o CONTRATANTE nenhuma exceção, restrição, alegação de descumprimento total ou parcial, que tenha em relação ao subcontratado ou que este tenha contra ele.

2.2. São obrigações do CONTRATANTE, sem prejuízo de outras previstas neste instrumento e respectivos anexos:

2.2.1. Designar um funcionário como gestor do contrato e que servirá de contato junto à CONTRATADA para gestão, acompanhamento e esclarecimentos que porventura se fizerem necessários durante a vigência contratual;

2.2.2. Comunicar, por escrito, toda e qualquer orientação acerca do objeto contratado, excetuados os entendimentos verbais determinados pela urgência, que deverão ser confirmados, por escrito, no prazo de 02 (dois) dia úteis;

2.2.3. Fornecer e colocar à disposição da CONTRATADA todos os elementos e informações, proporcionando as condições que se fizerem necessários à execução do objeto;

2.2.4. Vistoriar os produtos e/ou serviços conforme sua necessidade e conveniência;

2.2.5. Acompanhar e fiscalizar a execução do objeto contratual, nos aspectos técnico, de segurança, de confiabilidade e quaisquer outros de seu interesse, através de pessoal próprio ou de terceiros designados para este fim;

2.2.6. Monitorar o prazo, quantidade, qualidade, e níveis dos produtos e/ou serviços, conforme o caso, podendo rejeitá-los no todo ou em parte, caso estejam comprovadamente em desacordo com o contratado, reservando-se ao direito de suspender o pagamento até que o objeto seja executado em conformidade com o contratado;

2.2.7. Notificar, formalmente, a CONTRATADA sobre as irregularidades observadas no cumprimento do contrato, possibilitando a CONTRATADA a regularização de tais pontos;

2.2.8. Solicitar a substituição de qualquer empregado e/ou preposto da CONTRATADA, desde que devidamente fundamentado, quando o objeto do contrato for a prestação de serviços e for verificada a falta de qualificação, zelo e dedicação na execução das tarefas, ou outros comportamentos que prejudiquem as atividades e resultados, objeto deste instrumento;

2.2.9. Efetuar os pagamentos devidos, de acordo com o estabelecido neste ajuste.

3. CLÁUSULA TERCEIRA – DA PROTEÇÃO DE DADOS

3.1. As partes comprometem-se a tratar os dados pessoais necessários para a execução do presente contrato em conformidade com a Lei Geral de Proteção de Dados/LGPD (Lei Federal nº 13.709/2018) e com as orientações da ANPD – Autoridade Nacional de Proteção de Dados.

3.1.1. Sempre que solicitado, a CONTRATADA deverá apresentar evidências documentadas da conformidade de suas atividades de tratamento de dados pessoais com a LGPD, tais como: Política de Privacidade e Tratamento de Dados Pessoais, Política de Segurança da Informação, Política de Respostas à Incidentes de Segurança da Informação, canal de atendimento ao titular de dados pessoais e documento de nomeação do Encarregado pelo Tratamento de Dados Pessoais (DPO).

3.1.2. A CONTRATADA compromete-se a indicar Encarregado de Dados ou pessoa responsável por responder a avaliação de fornecedores ("*due diligence* LGPD") do CONTRATANTE, sem prejuízo de submeter-se a auditoria para atestar a conformidade dos tratamentos dos dados pessoais, a critério exclusivo do CONTRATANTE.

3.2. A CONTRATADA está autorizada a utilizar os dados pessoais acessados exclusivamente para cumprir com o objeto deste contrato, cumprir com obrigações legais e para defesa em processos judiciais e administrativos, caso seja necessário.

3.2.1. No caso de descumprimento deste dever pela CONTRATADA esta assumirá a posição de controladora dos dados pessoais, nos termos da LGPD, assumindo integral e exclusiva responsabilidade pelo tratamento dos dados pessoais, devendo manter o CONTRATANTE totalmente isento de quaisquer ônus, reclamações, processos, sanções e condenações decorrentes desses tratamentos.

3.3. A CONTRATADA está proibida de usar as informações pessoais que tiver acesso em razão do contrato em questão para: (i) interesse próprio, (ii) enriquecimento de sua base de dados, (iii) execução de contratos firmados com terceiros e (iv) divulgação dos seus produtos e serviços, sob pena de multa por violação contratual, notificação para a ANPD-Autoridade Nacional de Proteção de Dados Pessoais, além da obrigação de indenizar todos os prejuízos causados ao Sebrae por violação desta obrigação.

3.4. Estando autorizada a subcontratação no respectivo Termo de Referência (TR), a CONTRATADA está autorizada a compartilhar os dados pessoais com seus subcontratados apenas quando delegar a execução de alguma das etapas do contrato firmado com o CONTRATANTE.

3.4.1. A CONTRATADA deve informar o CONTRATANTE os seus subcontratados. Deve ser compartilhado o mínimo necessário para cumprir com a etapa a ser executada pelo subcontratado.

3.4.2. É dever da CONTRADADA garantir a confidencialidade e segurança deste compartilhamento, bem como instruir, exigir e fiscalizar o subcontratado para que este também observe todas as regras e limitações determinadas neste instrumento.

3.4.3. A CONTRATADA assume a responsabilidade pela violação deste instrumento, da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados/LGPD) e das orientações da ANPD -Autoridade Nacional de Proteção de dados Pessoais- cometidas por seus subcontratados durante o tratamento dos dados pessoais compartilhados pelo Sebrae.

3.5. As partes comprometem-se a prestar mútuo auxílio para atenderem os direitos dos titulares de dados pessoais dentro do prazo legal.

3.6. Na ocorrência de incidentes envolvendo as informações pessoais dos clientes do CONTRATANTE, a CONTATADA deverá comunicar o CONTRATANTE no prazo de 48 horas, a contar do conhecimento do incidente. Esta comunicação deverá conter todos os elementos do §1º art. 48, LGPD e as orientações da ANPD. A comunicação deve ser encaminhada para o/a Encarregado(a) de Dados Pessoais do CONTRATANTE (dpo@sebraesp.com.br).

3.6.1. Considera-se incidente o evento que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais, decorrente de ações voluntárias ou acidentais, que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados.

3.7. Qualquer violação à lei protetiva dos dados pessoais, não se limitando a Lei Geral de Proteção de Dados Pessoais/LGPD, e às orientações da ANPD -Autoridade Nacional de Proteção de Dados – praticada pela CONTATADA sujeita-se a rescisão imediata do contrato por culpa exclusiva desta, multa por descumprimento contratual e ao ressarcimento de todos os prejuízos materiais e morais causados ao CONTRATANTE.

3.8. Encerrado o contrato entre as partes, a CONTRATADA está proibida de manter os dados pessoais no seu ambiente, inclusive backup e ambientes externos, exceto o eventualmente necessário para o cumprimento de obrigações legais e a defesa em processos judiciais e administrativos. As informações devem ser descartadas de forma segura e definitiva, com técnicas que impeçam a sua recuperação tão logo sejam superadas as finalidades que legitimam o seu armazenamento.

3.8.1. Se solicitado, a CONTRATADA deverá fornecer declaração que ateste o descarte dos dados, as técnicas utilizadas e os ambientes físicos e tecnológicos que passaram pelo processo de descarte definitivo.

3.9. É parte integrante deste contrato as obrigações previstas no respectivo Termo de Referência.

4. CLÁUSULA QUARTA – DAS INFORMAÇÕES CONFIDENCIAIS

4.1. Consideram-se "Informações Confidenciais" todas as informações, dados, documentos, comunicações e conhecimentos técnicos ou comerciais de qualquer natureza, fornecidos, comunicados, transmitidos ou revelados por

uma das partes contratantes à outra, seja de forma verbal, escrita, eletrônica, por fax, desenhos, gráficos ou qualquer outra forma de transmissão, que se refiram, direta ou indiretamente, às atividades, operações, processos, métodos, técnicas, produtos, serviços, estratégias, planos de negócios, know-how, estudos, pesquisas, desenvolvimentos, invenções, patentes, marcas, logotipos, direitos autorais, informações financeiras, comerciais ou técnicas, e qualquer outra informação de propriedade ou interesse da parte reveladora.

4.2. A parte receptora se compromete a:

4.2.1. Utilizar as Informações Confidenciais exclusivamente para os fins para os quais foram fornecidas ou comunicadas;

4.2.2. Manter as Informações Confidenciais em estrito sigilo e não as divulgar, reproduzir, copiar, publicar ou compartilhar, seja de forma parcial ou total, com terceiros, sem o prévio consentimento escrito da Parte reveladora;

4.2.3. Empregar todos os esforços razoáveis para proteger as Informações Confidenciais, garantindo sua segurança e evitando sua divulgação não autorizada, inclusive por terceiros;

4.2.4. Restringir o acesso às Informações Confidenciais apenas aos funcionários, colaboradores ou terceiros que necessitem conhecer tais informações para o cumprimento das obrigações previstas neste contrato, sempre orientando-os quanto à confidencialidade e proibindo sua divulgação a terceiros;

4.3. As obrigações previstas nesta cláusula não se aplicam às informações que:

4.3.1. Ao tempo de sua transmissão, ou posteriormente, sejam ou venham a ser de domínio público, conforme evidenciado por publicações idôneas, desde que sua divulgação não tenha sido causada pela parte receptora;

4.3.2. Estiverem na posse legal da parte receptora por ocasião da divulgação, desde que tenham sido recebidas legitimamente de terceiro (que não seja a outra parte), sem violação de obrigação legal e/ou obrigação de sigilo assumida com a parte reveladora;

4.3.3. Forem independentemente desenvolvidas pela Parte receptora, sem utilização direta ou indireta de informações confidenciais;

4.3.4. Forem necessariamente divulgadas no cumprimento de ordem judicial, ficando ressalvado que a parte receptora deverá, nesse caso, avisar a outra parte, imediatamente, por escrito, para que a esta seja dada a oportunidade de se opor à revelação e/ou tomar medidas legítimas e razoáveis para evitar ou minimizar o alcance dessa divulgação.

4.3.5. Ao tempo de sua transmissão, forem invadidas e conhecidas por terceiros, diversos das partes deste instrumento, sem que haja culpa da parte receptora.

4.4. Assumirá inteira responsabilidade por qualquer forma de divulgação não autorizada, a parte que divulgar as informações confidenciais de que trata essa cláusula, ainda que feita por seus acionistas, diretores, empregados, prestadores de serviços ou fornecedores a ela vinculados.

4.5. A parte que infringir a confidencialidade indenizará a outra parte por todas as perdas e danos derivados da quebra de sigilo e confidencialidade com relação às informações confidenciais.

4.6. A pedido da parte que disponibilizou as informações confidenciais, a parte que as recebeu devolverá à mesma, imediatamente, todos os documentos e outras manifestações corpóreas das informações confidenciais recebidas nos termos deste instrumento e todas as cópias e reproduções a que se referirem.

4.7. O término da contratação não eximirá as partes das obrigações por elas assumidas quanto ao sigilo e confidencialidade em relação às informações confidenciais a que tiveram acesso durante a execução do objeto.

4.8. As disposições dessa cláusula não deverão ser interpretadas implicitamente, por presunção, analogia ou de outra forma, como concessão de licença por uma das partes à outra para fazer, mandar fazer, usar ou vender qualquer produto e/ou serviço utilizando as informações confidenciais, ou como licença nos termos de qualquer patente, pedido de registro de patente, modelo de utilidade, direito autoral ou qualquer outro direito de propriedade industrial ou intelectual cobrindo o mesmo.

5. CLÁUSULA QUINTA – DA COMPOSIÇÃO DO VALOR DESTE CONTRATO

5.1. O valor total deste contrato é de R$ 2.309.500,00 (Dois milhões, trezentos e nove mil e quinhentos reais), sendo assim composto:

(A) **ITEM**	**(B)** **DESCRIÇÃO**	**(C)** **FORMA DE PAGAMENTO**	**(D)** **UNIDADE**	**(E)** **QTD TOTAL PARA REGISTRO**	**(F)** **VALOR UNITÁRIO**	**(G)** **VALOR TOTAL G = E x F**
1	Solução de Gerenciamento de Exposição Contínua a Ameaças. Período de subscrição = 24 meses	Parcelas Anuais	Unidade	1	R$ 798.000,00	R$ 798.000,00
2	Licenciamento da Capacidade de Validação de Brechas e Simulações de Ataques. Período de subscrição = 24 meses	Parcelas Anuais	Usuário	2.600	R$ 280,00	R$ 728.000,00
3	Licenciamento da Capacidade de Gestão de Superfície de Ataque Externo. Período de subscrição = 24 meses	Parcelas Anuais	Ativo	2.500	R$ 227,00	R$ 567.500,00
4	Serviço de suporte técnico especializado da solução.	Mensal	Mês	24	R$ 9.000,00	R$ 216.000,00
Valor Total: R$ 2.309.500,00 (Dois milhões, trezentos e nove mil e quinhentos reais)						

5.2. O (s) valor (es) ora descrito (s) abarca (m) todas as despesas diretas e indiretas e quaisquer outras obrigações ou despesas necessárias à perfeita execução do objeto contratual.

6. CLÁUSULA SEXTA – DA FORMA DE PAGAMENTO

6.1. Após o **recebimento do objeto,** a CONTRATADA deverá encaminhar **a nota fiscal,** para conferência, validação e pagamento.

6.2. A CONTRATADA deverá emitir a nota fiscal e encaminhá-la ao SEBRAE-SP até o dia 17 (dezessete) do mês subsequente ao da prestação dos serviços e/ou entrega dos produtos, acompanhada dos documentos que comprovem a regularidade fiscal e trabalhista (Certidões Negativas de Débitos com o INSS, FGTS e comprovação de regularidade junto às receitas federal, estadual e municipal do domicílio ou sede da CONTRATADA).

6.3. O pagamento será efetuado em até 30 (trinta) dias após o aceite definitivo da nota fiscal/fatura pelo SEBRAE-SP, condicionado à homologação do Produto/Serviço entregue, ao ateste das notas fiscais e à apresentação de relatório de prestação de serviços, conforme aplicável.

6.4. O SEBRAE-SP não aceitará recibo como documento fiscal, exceto nos casos estritamente legais de dispensa de emissão de nota fiscal, devidamente comprovado pela CONTRATADA.

6.5. O SEBRAE-SP reserva-se o direito de suspender o pagamento nos seguintes casos:

a) Se os serviços não estiverem sendo prestados conforme o proposto e contratado;
b) Se houver erros ou incorreções na documentação fiscal apresentada, caso em que a CONTRATADA deverá providenciar a regularização, reiniciando-se o prazo de pagamento após a reapresentação correta.

6.6. O pagamento será efetuado mediante crédito em conta corrente de titularidade da CONTRATADA, que deverá indicar o nome do banco, número e nome da agência, número da conta corrente de sua titularidade e tipo de conta, conforme modelo do ANEXO – DECLARAÇÃO DE DADOS BANCÁRIOS.

6.7. Quaisquer despesas decorrentes de transações bancárias, inclusive a devolução de pagamento por inconsistência de dados bancários, serão de responsabilidade da CONTRATADA.

6.8. O SEBRAE-SP poderá deduzir do montante a ser pago eventuais multas, indenizações ou valores decorrentes de glosas, conforme previsto neste contrato

6.9. Nos casos de eventuais atrasos no pagamento, desde que a CONTRATADA não tenha concorrido, de alguma forma, para o atraso, o CONTRATANTE pagará encargos moratórios calculados conforme a fórmula abaixo:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,000166667, assim apurado: I = (TX) I = (6 / 100) I = 0,000166667 360 TX = Percentual da taxa anual = 6%

7. CLÁUSULA SÉTIMA – DO RECEBIMENTO DO OBJETO – PROVISÓRIO E DEFINITIVO

7.1. O objeto do presente contrato será recebido nas seguintes condições:

7.1.1. Recebimento Provisório: o responsável pelo acompanhamento e fiscalização do contrato realizará o recebimento provisório em até 15 (quinze) dias do recebimento, juntamente com os documentos comprobatórios para sua conferência e aceite, formalizando o seu recebimento para posterior verificação da conformidade do material/serviço com as exigências contratuais.

7.1.2. Recebimento Definitivo: O recebimento definitivo total dos produtos contratados apenas ocorrerá por ocasião de sua montagem e seu aceite final emitido pelo SEBRAE-SP, mediante a emissão do Termo de Recebimento Definitivo, acompanhado de relatório detalhado que comprove as condições de execução contratual.

7.1.3. O objeto do contrato poderá ser rejeitado, no todo ou em parte, caso esteja em desacordo com as especificações e condições estabelecidas neste contrato, sendo obrigação da contratada as correções necessárias, as suas expensas, sem que neste prazo ocorra a obrigação de pagamento.

7.1.4. O recebimento provisório ou definitivo não exime o contratado das responsabilidades civil, ético-profissional, e outras estabelecidas pela lei ou por este contrato, incluindo a solidez, segurança, e perfeita execução do objeto contratado.

7.1.5. Salvo disposição em contrário, todos os ensaios, testes e provas necessários para a verificação da boa execução do objeto contratado serão de responsabilidade e custeio da contratada, conforme normas técnicas oficiais aplicáveis, se for o caso.

7.1.6. A CONTRATADA garante que os produtos fornecidos e/ou os serviços prestados neste contrato estão em conformidade com padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme estabelecido nas especificações técnicas e normas aplicáveis, por 90 (noventa) dias além do prazo estabelecido no art. 26 do Código de Defesa do Consumidor (CDC), instituído pela Lei nº 8.078/1990.

7.1.7. Durante o período de garantia legal dos produtos fornecidos e/ou dos serviços prestados, a CONTRATADA compromete-se a prestar assistência técnica necessária para correção de eventuais defeitos ou vícios que comprometam a qualidade, segurança, durabilidade e desempenho dos produtos ou serviços.

7.1.8. Caso seja necessário, a CONTRATADA compromete-se a substituir componentes defeituosos ou produtos inteiros ou por outros de mesma espécie, marca e modelo, em perfeitas condições de uso, ou a refazer serviços não recebidos, sem qualquer ônus adicional ao Contratante.

8. CLÁUSULA OITAVA – DA VIGÊNCIA E DO PRAZO DE EXECUÇÃO

8.1. A vigência contratual será de **24 (vinte e quatro) meses**, contados da data da conclusão das assinaturas dos representantes legais das partes, podendo ser prorrogada, a critério do CONTRATANTE, de acordo com os permissivos do Regulamento de Licitações e de Contratos do Sistema SEBRAE.

8.2. A decisão de prorrogação do contrato é exclusiva do CONTRATANTE, sendo necessária a anuência da CONTRATADA, em razão da liberalidade contratual.

8.3. Caso a CONTRATADA não tenha interesse em prorrogar o contrato, deverá manifestar sua intenção por escrito, com antecedência mínima de 60 (sessenta) dias antes do término da vigência contratual, sob pena de aplicação de sanção contratual.

8.4. A prorrogação do contrato estará condicionada à justificativa da manutenção do interesse no objeto do contrato pelo CONTRATANTE e à comprovação da vantajosidade econômica.

8.5. A cada 12 (doze) meses, poderá haver reajuste com base no IPCA.

9. CLÁUSULA NONA – DAS PENALIDADES

9.1. Comete infração administrativa nos termos da legislação vigente, do Regulamento de Licitações e Contratos do Sistema SEBRAE e do presente instrumento contratual e respectivos anexos, a(s) Contratada(s) que:

9.1.1. der causa à inexecução parcial do contrato;

9.1.2. der causa à inexecução total do contrato;

9.1.3. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

9.1.4. descumprir o prazo para notificação do não interesse em prorrogar a vigência contratual previsto na subcláusula 8.3.

9.1.5. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

9.1.6. praticar ato fraudulento na execução do contrato;

9.1.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

9.1.8. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

9.2.1. Advertência escrita, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

9.2.2. **Suspensão do direito de licitar e/ou contratar com o CONTRATANTE pelo prazo de até 03 (três) anos**, observada a gravidade da conduta da contratada, bem como os princípios da proporcionalidade e razoabilidade, assim como as demais sanções no caso concreto, e conforme regra geral abaixo:

9.2.2.1. 12 (doze) meses, nos casos de: aplicação de duas ou mais penas de advertência, em um intervalo de tempo inferior a 12 (doze) meses, sem que o fornecedor tenha adotado as medidas corretivas no prazo determinado pelo CONTRATANTE, alteração de quantidade ou qualidade do produto ou serviço fornecido;

9.2.2.2. De 13 (treze) até 24 (vinte e quatro) meses, nos casos de: retardamento imotivado de parcela significativa da execução da obra, de serviço ou do fornecimento de bens;

9.2.2.3. 36 (trinta e seis) meses, nos casos de: entregar como verdadeira, mercadoria falsificada, adulterada, deteriorada ou danificada; paralisação de serviço, de obra ou de fornecimento de bens sem justa fundamentação e prévia comunicação ao CONTRATANTE; praticar ato ilícito visando a frustrar os objetivos da licitação.

9.2.3. **Suspensão do direito de licitar e contratar com o Sistema SEBRAE, pelo prazo mínimo de 4 (quatro) e máximo de 6 (seis) anos**, nas seguintes hipóteses, nas hipóteses descritas 9.1.5, 9.1.6, 9.1.7 e 9.1.8, hipóteses nas quais, após o processamento do processo sancionador no âmbito do CONTRATANTE, os autos serão encaminhados para deliberação final do SEBRAE Nacional.

9.2.4. **Multa:**

9.2.4.1.1. **Moratória de** 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias.

9.2.4.2. **Compensatória de:**

9.2.4.2.1. 20% (vinte por cento) sobre o valor da parcela inadimplida para a infração prevista no subitem 9.1.1.

9.2.4.2.2. 20% (vinte por cento) sobre o valor total do contrato para a infração prevista no subitem 9.1.2;

9.2.4.2.3. 20% (vinte por cento) sobre o valor da parcela inadimplida para a infração prevista no subitem 9.1.3;

9.2.4.2.4. 1% (um por cento) sobre o valor total do contrato para a infração prevista no subitem 9.1.4.

9.2.4.2.5. 20% (vinte por cento) sobre o valor total do contrato para as infrações previstas nos subitens 9.1.5, 9.1.6, 9.1.7 e 9.1.8.

9.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.

9.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa.

9.5. A aplicação de qualquer das sanções previstas realizar-se-á por processo administrativo, assegurado o contraditório e a ampla defesa à CONTRATADA.

9.6. Para fins de aplicação das penalidades descritas nesta cláusula, a cada infração cometida a CONTRATADA será notificada para apresentação de defesa, no prazo de até 5 (cinco) dias úteis, contados a partir do dia útil subsequente ao recebimento da notificação.

9.7. Na aplicação das sanções serão considerados:

9.7.1. a natureza e a gravidade da infração cometida;

9.7.2. as peculiaridades do caso concreto;

9.7.3. os danos que dela provierem ao CONTRATANTE;

9.7.4. o caráter pedagógico da sanção.

9.8. As multas devidas e/ou prejuízos causados ao CONTRATANTE serão deduzidos das faturas devidas à CONTRATADA, ou deduzidos da garantia, caso esta tenha sido exigida.

9.8.1. Se os valores das faturas e da garantia contratual forem insuficientes, fica a CONTRATADA obrigada a recolher em favor do CONTRATANTE a importância devida no prazo de 15 (quinze) dias, contados da comunicação oficial.

9.8.2. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser complementada no prazo de até 10 (dez) dias úteis, contados da solicitação do CONTRATANTE.

9.9. Em qualquer caso, fica a CONTRATADA responsável, ainda, pelas perdas e danos adicionais, valendo os percentuais de multa ora estabelecidos tão somente como mínimo legal, nos termos do artigo 416, parágrafo único, do Código Civil, sem qualquer prejuízo do cumprimento da obrigação principal.

10. CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES TRABALHISTAS

10.1. O presente contrato não implica, para o CONTRATANTE, vínculo ou obrigação trabalhista, direta ou indireta, de qualquer natureza, obrigando-se ainda a CONTRATADA a manter o CONTRATANTE a salvo de qualquer litígio, assumindo todas as obrigações fiscais, trabalhistas, previdenciárias, sociais e seguros referentes ao pessoal utilizado para o cumprimento do presente ajuste, inclusive com relação a terceiros contratados.

10.2. A CONTRATADA responsabiliza-se, de forma única e exclusiva, por quaisquer acidentes de que possam ser vítimas seus empregados e prepostos, quando nas dependências do CONTRATANTE, ou em qualquer outro local onde estejam prestando os serviços, devendo adotar as providências que, a respeito, exigir a legislação em vigor.

10.3. A CONTRATADA responsabiliza-se pelas despesas da defesa, inclusive por custas e honorários advocatícios, bem como pelo cumprimento das decisões judiciais em reclamações trabalhistas eventualmente propostas por seus empregados, prepostos, ex-empregados ou terceiros envolvendo o CONTRATANTE, isentando ainda o CONTRATANTE de quaisquer responsabilidades e/ou ônus decorrentes direta ou indiretamente dos referidos processos judiciais;

10.4. A CONTRATADA responsabiliza-se civil e criminalmente perante o CONTRATANTE e terceiros por eventuais prejuízos, danos ou delitos causados por seus empregados, prepostos e/ou contratados, decorrentes de erro, culpa ou dolo, por demora ou omissão, na prestação dos serviços de sua responsabilidade, devendo indenizar todos os prejuízos ocasionados.

11. CLÁUSULA DÉCIMA PRIMEIRA – DO CÓDIGO DE ÉTICA

11.1. A CONTRATADA compromete-se a respeitar, cumprir e fazer cumprir, no que couber, o “Código de Ética do Sistema SEBRAE” que se encontra disponível no site do SEBRAE no endereço eletrônico www.sebrae.com.br, Ouvidoria, opção Código de Ética do SEBRAE.

12. CLÁUSULA DÉCIMA SEGUNDA – DA ANTICORRUPÇÃO

12.1. As partes concordam que executarão as obrigações contidas neste contrato de forma ética e de acordo com os princípios aplicáveis ao Sistema SEBRAE, previstos no artigo 2º do Regulamento de Licitações e Contratos.

12.2. A CONTRATADA assume que é expressamente contrária à prática de atos que atentem contra o patrimônio e a imagem do Sistema SEBRAE.

12.3. Nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis nacionais, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma que não relacionada a este contrato, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

12.4. As partes se comprometem a estabelecer, de forma clara e precisa, os deveres e as obrigações de seus agentes e/ou empregados em questões comerciais, para que estejam sempre em conformidade com as leis, as normas vigentes e as determinações deste contrato.

13. CLÁUSULA DÉCIMA TERCEIRA – DAS ALTERAÇÕES

13.1. Este CONTRATO poderá ser alterado por meio de Termos Aditivos, objetivando promover os acréscimos ou supressões que se fizerem necessários.

13.2. Os acréscimos que se fizerem necessários no objeto do contrato estão limitados a 50% (cinquenta por cento) do valor global atualizado do contrato, mediante justificativa.

13.3. A supressão poderá ser realizada no limite estabelecido entre as partes.

14. CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. O CONTRATO poderá ser rescindido por inexecução total ou parcial, por infração legal ou por descumprimento de qualquer uma de suas cláusulas.

14.2. Os casos de rescisão contratual serão formalmente motivados, assegurados o contraditório e a ampla defesa.

14.3. A rescisão do contrato poderá ser:

14.3.1. Por ato unilateral do CONTRATANTE, nos casos previstos no contrato;

14.3.2. Amigável, por acordo entre as partes, mediante a assinatura de termo de distrato; e

14.3.3. Judicial, nos termos da legislação.

15. CLÁUSULA DÉCIMA QUINTA – DAS DISPOSIÇÕES FINAIS

15.1. As despesas decorrentes deste contrato onerarão as verbas do CONTRATANTE, consignadas em seu orçamento.

15.2. Fazem parte do contrato, independentemente de transcrição, todas as condições constantes do edital que lhe deu origem, seus anexos e a proposta apresentada pela CONTRATADA, permanecendo, caso haja conflito, as disposições constantes deste instrumento contratual.

15.3. As solicitações de Atestado de Capacidade Técnica, relativo à execução do contrato, deverão ser formulados no prazo máximo de 12 (doze) meses após o encerramento da vigência contratual ao gestor do contrato, indicando a razão social, CNPJ e o número do instrumento contratual.

15.4. No caso de contrato de escopo, envolvendo a conclusão de um objeto específico, o atestado somente será emitido após o término da execução dos serviços ou da entrega dos produtos contratados. No caso de contrato de execução continuada, o atestado somente será emitido após o final da vigência inicialmente pactuada.

16. CLÁUSULA DÉCIMA SEXTA – DO FORO

16.1. Fica eleito o Foro da Comarca da Capital do Estado de São Paulo, com expressa renúncia de qualquer outro, por mais especial ou privilegiado que seja ou venha a ser, para dirimir quaisquer dúvidas ou litígios decorrentes do presente ajuste.

As Partes declaram que o presente instrumento, incluindo todas as páginas e eventuais anexos, todas formatadas por meio digital, representam a integralidade dos termos entre elas acordados.
E, por estarem de acordo, as partes expressamente concordam em utilizar e reconhecem como válida a plataforma de assinaturas do SEBRAE (https://www.sgolite.sebrae.com.br/PortalAssinaturaDigital/#/), admitindo válidas as assinaturas realizadas eletronicamente.

São Paulo,

REINALDO PEDRO CORREA
Diretor de Administração e Finanças
SEBRAE-SP

RODRIGO GARCIA MEDEIROS
LAYER TECNOLOGIA DA INFORMAÇÃO LTDA

CARLOS KAZUNARI TAKAHASHI
Gerente da Unidade Tecnologia Corporativa
SEBRAE-SP

VICTOR ARAUJO FREIRE
LAYER TECNOLOGIA DA INFORMAÇÃO LTDA

TESTEMUNHAS:

Nome: Eliezer Benevides

Nome: Cicera Mota

ANEXO DO TERMO DE REFERÊNCIA
Processo 0084/2025

1. OBJETO

1.1. Registro de Preços para contratação de empresa para o fornecimento de Solução de Gerenciamento de Exposição Contínua a Ameaças Cibernéticas, com serviços de implantação, suporte técnico e repasse de conhecimento, para atendimento as demandas do SEBRAE-SP.

2. JUSTIFICATIVA

2.1. A solução de Breach and Attack Simulation (BAS) será utilizada para aprimorar continuamente os controles de segurança do ambiente, permitindo a identificação proativa de vulnerabilidades e a validação da efetividade das defesas implementadas.

2.2. Instituições modernas dependem fortemente de tecnologia e segurança cibernética para suas operações.

2.3. A falta de disponibilidade ou segurança nesses sistemas pode prejudicar os negócios e a confiança pública.

2.4. O SEBRAE-SP busca adotar soluções robustas de cibersegurança, incluindo simulações de ataques para avaliar a eficácia das defesas.

2.5. Diante das limitações das práticas manuais, o Gerenciamento Contínuo de Exposição a Ameaças Cibernéticas é essencial.

2.6. Essa abordagem, mencionada pelo Gartner, automatiza testes de segurança e identifica vulnerabilidades em tempo real, permitindo simular ataques APTs e malware. Portanto, a aquisição dessa solução é recomendada para garantir a proteção de informações corporativas, dados sensíveis e fortalecer a capacidade de resposta a incidentes em um cenário crescente de ameaças cibernéticas.

3. ESPECIFICAÇÕES TÉCNICAS

3.1. A prestação dos serviços deverá ser executada de acordo com as regras e procedimentos definidos no ANEXO – ESPECIFICAÇÕES TÉCNICAS MÍNIMAS E OBRIGATÓRIAS, sendo:

3.1.1. **Item 1** - Solução de Gerenciamento de Exposição Contínua a Ameaças - Período de subscrição por 24 meses.

3.1.2. **Item 2** - Licenciamento da Capacidade de Validação de Brechas e Simulações de Ataques - Período de subscrição por 24 meses.

3.1.3. **Item 3** - Licenciamento da Capacidade de Gestão de Superfície de Ataque Externo. - Período de subscrição por 24 meses.

3.1.4. **Item 4** - Serviço de suporte técnico especializado da solução.

3.2. A CONTRATADA deverá executar o contrato em conformidade com a Legislação vigente e as determinações de órgãos reguladores/fiscalizadores, em especial com a Lei 12.965/2014 (Marco Civil da Internet) e o Decreto 8.771/2016 que regulamenta a referida Lei, e também com as orientações das entidades de padronização e normatização;

3.3. Assegurar o cumprimento de todas as normas de segurança e regulamentos internos do SEBRAE-SP por parte dos profissionais alocados para a execução do contrato;

3.4. Providenciar o ambiente e recursos necessários para a execução do contrato, tais como, mas não limitadamente, materiais, cabeamento, conectores, equipamentos, softwares referentes ao objeto e infraestrutura necessária, arcando com eventuais custos decorrentes;

3.5. Manter a sua regularidade fiscal durante todo o período de execução do contrato;

3.6. Responsabilizar-se integralmente pela disponibilização de produtos e serviços à CONTRATADA, nos termos da legislação vigente, de modo que sejam realizados com esmero e perfeição, sob sua inteira e exclusiva responsabilidade, obedecendo às normas e rotinas do SEBRAE, em especial às que digam respeito à segurança, à confiabilidade e à integridade;

3.7. Responder por quaisquer danos causados ao SEBRAE-SP ou a terceiros, decorrentes de sua responsabilidade ou dolo na execução do contrato;

3.8. Suporte

3.8.1. Indicar preposto que será o responsável pelo relacionamento com o SEBRAE-SP com experiência em coordenação e supervisão de contratos e projetos.

3.8.2. Deverá possuir os conhecimentos e a capacidade profissional necessária, deverá ter competência para resolver imediatamente todo e qualquer assunto relacionado com os itens contratados. Este representante deverá estar disponível nas dependências do SEBRAE, quando necessário, para acompanhamento das demandas contratadas;

3.8.3. Fornecer a descrição técnica detalhada e a documentação técnica em meio digital (incluindo todos os manuais) de todos os equipamentos e demais ativos necessários para execução do contrato e se responsabilizar pela instalação e manutenção de toda a infraestrutura da solução, a fim de garantir os níveis de serviços contratados, devendo seu custo estar contemplado nos preços apresentados em sua proposta;

3.8.4. Entregar ao SEBRAE-SP documento descrevendo toda a sua estrutura interna de equipe, que estará alocada para atendimento ao SEBRAE-SP, constando as funções de cada componente dessa estrutura, identificando todas as pessoas envolvidas com o atendimento ao SEBRAE-SP, formas de contato e todos os procedimentos a serem seguidos, em caso de necessidade de encaminhamento de alguma solicitação.

3.9. DA TRANSIÇÃO CONTRATUAL

3.9.1. A CONTRATADA deverá apresentar em um prazo máximo de 60 (sessenta) dias antes do término da vigência do contrato, um plano para transferência de conhecimentos e tecnologias, a ser aprovado pelo SEBRAE, para a próxima empresa que vier a prestar os mesmos serviços ao SEBRAE e/ou para empregados do próprio SEBRAE.

3.9.2. Neste prazo, consideram-se 30 (trinta) dias para a execução do plano e os últimos 30 (trinta) dias para a verificação da qualidade da transição.

3.9.3. §1° O plano de transferência deverá conter, pelo menos, a revisão de toda a documentação gerada de todos os itens executados, acrescido de outros documentos que, não sendo artefatos previstos em metodologia, sejam adequados ao correto entendimento do item executado, e necessariamente capacitações, que deverão ocorrer no período de execução do plano, aos empregados do SEBRAE e/ou para a próxima empresa que vier a prestar o mesmo serviço ao SEBRAE.

3.9.4. §2° Eventual necessidade de utilização de recursos do SEBRAE poderá ser solicitada pela CONTRATADA para execução do plano de transferência.

3.9.5. §3° Os serviços prestados na execução do plano de transferência de conhecimentos e tecnologias estão incluídos nos serviços ora contratados, não cabendo ao SEBRAE qualquer remuneração adicional.

3.9.6. §4° As falhas identificadas no período final de verificação da qualidade da transição, como a não cooperação ou retenção de qualquer informação ou dados solicitados pelo SEBRAE, que venham a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços, poderão ensejar aplicação das sanções previstas na Cláusula Penal do contrato.

3.10. OBSERVÂNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

3.10.1. A CONTRATADA obriga-se à aceitação e ao cumprimento da Política de Segurança de Tecnologia de Informação e Comunicação do SEBRAE, bem como dos seus documentos complementares.

3.10.2. § 1º A CONTRATADA compromete-se a:

3.10.2.1. Preservar a confidencialidade, a integridade e a disponibilidade das informações obtidas durante a vigência da relação jurídica com o SEBRAE, mesmo após o seu término;

3.10.2.2. informar imediatamente ao gestor do contrato a respeito de qualquer falha, incidente ou anormalidade dos ativos de Tecnologia de Informação e Comunicação do SEBRAE-SP;

3.10.3. § 2° Os recursos de Tecnologia de Informação e Comunicação, assim como os softwares trazidos pela CONTRATADA para o SEBRAE-SP, são de exclusiva responsabilidade da CONTRATADA.

3.10.4. § 3° A violação a esta cláusula resultará em medidas cabíveis, inclusive judiciais, além das previstas na cláusula penal deste instrumento.

3.11. EQUIPE MÍNIMA

3.11.1. É de responsabilidade da contratada executar o contrato sob a sua exclusiva responsabilidade, utilizando profissionais qualificados, tecnicamente aptos, habilitados e treinados para atender, com alta qualidade e nível técnico, às especificações e prazos.

3.11.2. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

3.11.2.1. Experiência comprovada de no mínimo 06 (seis) meses na área de Tecnologia da Informação;

3.11.2.2. Conhecimento avançado na solução, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado.

4. LOCAL, FORMA E CRONOGRAMA DE ENTREGA, EXECUÇÃO E PAGAMENTO

4.1. Do Local

4.1.1. A solução será disponibilizada na modalidade “Software as a Service – Saas” (Software como Serviço), ou seja, utilizaremos a infraestrutura de nuvem da empresa fornecedora da solução.

4.2. Da Forma – Reunião de Briefing

4.2.1. Após a assinatura do contrato, em um prazo de até 05 (cinco) dias, deverá ser realizada reunião inicial entre a CONTRATADA e o Gestor do Contrato do SEBRAE/SP para acertos iniciais quanto a prestação de serviço e definição das fases do cronograma para atendimento.

4.2.2. Outras reuniões poderão ser agendadas pelo SEBRAE-SP, quando houver formalização da solicitação, necessidade de ajustes em relação à execução do objeto, dentre outras necessidades.

4.2.3. As reuniões poderão ocorrer de forma remota (online) ou presencial, a ser realizada na sede do SEBRAE-SP, localizado à Av. Vergueiro, 1.117 – Liberdade – São Paulo/SP, ou em outro local a ser definido em concordância com a contratada e o SEBRAE-SP.

4.2.4. A entrega do objeto deste contrato será demandada pelo SEBRAE-SP por meio de Ordens de Fornecimento e/ou Serviços, a serem emitidas pela respectiva Unidade Tecnologia Corporativa.

4.2.5. §1º Os pedidos serão feitos de acordo com a necessidade do SEBRAE, não obrigando o SEBRAE a realizá-los em sua totalidade. Não caberá à CONTRATATADA qualquer tipo de indenização ou reparação neste sentido.

4.2.6. §2º As Ordens de Fornecimento/Serviços deverão obrigatoriamente: identificar os serviços/item do objeto da licitação a serem executados/entregues, o prazo de entrega e local de entrega, bem como, o técnico da respectiva Unidade Tecnologia Corporativa do SEBRAE que será responsável pela gestão, avaliação e emissão do Termo de Aceite dos serviços prestados e das faturas decorrentes.

4.3. DO CRONOGRAMA DE ENTREGA, EXECUÇÃO

Evento	Descrição do Evento	Prazo Máximo	% a pagar
Todos os Itens			
1	Assinatura do contrato.	Dia D_1	0%
2	Reunião Inicial e emissão de Ordem de Serviços.	Dia D_2, sendo D_2 conforme demanda do SEBRAE	0%
3	Entrega do Projeto Executivo de Implementação – PEI.	D_2 + 15 dias	0%
4	Itens 01 a 03 :Ativação do licenciamento de software demandado por OS.	D_2 + 30 dias	1º ano: 50% do valor total de cada item demandado por Ordem de Serviço - OS. 2º ano: 50% do valor total de cada item demandado por Ordem de Serviço - OS.
5	ITEM 04: Execução dos serviços referentes ao serviço de suporte técnico da solução.	D_2 + 30 dias	100% do valor mensal do item.

* Não há óbice na antecipação dos prazos de entrega e execução pela CONTRATADA, bem como da antecipação dos prazos de recebimento, aceitação e pagamento do SEBRAE-SP desde que obedecidas as demais condições deste instrumento.

4.4. FORMA DE PAGAMENTO

4.4.1. Para os Itens 1 - Solução de Gerenciamento de Exposição Contínua a Ameaças e 3 - Licenciamento da Capacidade de Gestão de Superfície de Ataque Externo o termo “2x Parcelas Anuais” define que o pagamento do valor total do item será realizado em 2 (duas) parcelas anuais, após a execução da Ordem de Fornecimento de Serviço (OS), ateste pelo fiscal e gestor do contrato e entrega da nota fiscal.

4.4.2. Para o Item 4 - Serviço de suporte técnico especializado da solução. o termo “Parcela Mensal” define que os pagamentos serão realizados em parcelas mensais, iguais e consecutivas, após a execução de cada Ordem de Serviço (OS), ateste pelo fiscal e gestor do contrato e entrega da nota fiscal.

4.4.3. Todos os pagamentos ocorrerão, somente após ateste pelo fiscal e gestor do contrato, nos termos do item “CRONOGRAMA DE ENTREGA, EXECUÇÃO E PAGAMENTO”, sem prejuízo as demais condições deste instrumento e seus anexos.

5. ACOMPANHAMENTO, FISCALIZAÇÃO E RECEBIMENTO

5.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do contrato.

5.2. As atividades de gestão e fiscalização da execução contratual serão realizadas de forma preventiva, rotineira e sistemática, pelo fiscal técnico do contrato designado pelo SEBRAE.

5.3. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

5.4. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento.

5.5. Quando solicitado, a CONTRATADA deverá fornecer ao SEBRAE-SP relatórios referentes aos serviços executados e /ou materiais entregues.

5.5.1. Os relatórios serão definidos em conjunto com a equipe técnica do SEBRAE-SP e poderão sofrer atualizações na medida em que o nível de controle dos serviços prestados se torne necessário.

5.6. O recebimento definitivo será realizado em até 15 (quinze) dias após o recebimento provisório.

5.6.1. O termo de recebimento definitivo obedecerá aos seguintes critérios:

5.6.1.1. SEBRAE-SP terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo, depois de finalizado o planejamento, customização e a instalação do ambiente;

5.6.1.2. A prestação dos serviços mensais iniciará somente a partir da emissão do termo de recebimento definitivo pelo SEBRAE;

5.6.1.3. Para todos os bens importados, caso necessário, por parte da CONTRATADA, que sejam instalados nas dependências do SISTEMA SEBRAE, será necessária a apresentação dos respectivos comprovantes de origem.

6. ESTIMATIVA DE CONSUMO

6.1. As estimativas de quantidades constituem mera previsão dimensionada, não estando o SEBRAE-SP obrigado a realizá-las em sua totalidade, não cabendo a CONTRATADA o direito de pleitear qualquer tipo de reparação e/ou indenização. Portanto, o SEBRAE-SP se reserva ao direito de, a seu critério, utilizar ou não as quantidades previstas.

6.2. A CONTRATADA terá direito somente ao pagamento em contraprestação às quantidades efetivamente consumidas, o que será comprovado através das entregas efetuadas pela CONTRATADA e aprovadas pelo SEBRAE-SP.

7. DOCUMENTAÇÃO ENTREGÁVEL

7.1. **Suporte - A** CONTRATADA deverá apresentar Relatório Técnico, ao final de cada atendimento, devidamente assinado por um representante do SEBRAE-SP.

7.1.1. **Para o ITEM 01:** Solução de Gerenciamento de Exposição Contínua a Ameaças.
7.1.1.1. Apresentar evidências da ativação da plataforma no formato SaaS.
7.1.1.2. Relatório as-built da ativação da plataforma em nome do SEBRAE.

7.1.2. **Para o ITEM 02:** Licenciamento da Capacidade de Validação de Brechas e Simulações de Ataques.

7.1.2.1. Relatório as-built com evidências da ativação na plataforma do ITEM 01 do volume de licenças adquiridas através do ITEM 02.

7.1.3. **Para o ITEM 03**: Licenciamento da Capacidade de Gestão de Superfície de Ataque Externo.

7.1.3.1. Relatório as-built com evidências da ativação na plataforma do ITEM 01 do volume de licenças adquiridas através do ITEM 03.

7.1.4. **Para o ITEM 04:** Serviço de suporte técnico especializado da solução.

7.1.4.1. Relatórios periódicos, minimamente mensais e trimestrais, com o detalhamento dos serviços executados.

8. ACORDO DE NÍVEL DE SERVIÇO (ANS)

8.1. Para acompanhamento e avaliação dos serviços pela CONTRATADA foram estabelecidos e utilizados Acordo de Níveis de Serviço (doravante denominados ANS) expressos como indicadores definidos para o processo.

8.2. O ANS deverá ser considerado e entendido pela CONTRATADA como um compromisso de qualidade que será assumido junto ao SEBRAE-SP. A análise dos resultados dos indicadores de nível de serviço poderá resultar na redução do valor pago pelos serviços prestados, caso a CONTRATADA não cumpra com seus compromissos na entrega dos serviços.

8.3. Com base no relatório e documentos solicitados, o SEBRAE-SP irá apurar os indicadores de ANS estabelecido neste instrumento.

8.4. **Indicadores:**

8.4.1. Os indicadores serão utilizados para acompanhamento dos serviços prestado e seu cumprimento indica que os serviços estão sendo entregues de acordo com a qualidade e desempenho esperados pelo SEBRAE-SP.

8.4.2. **Os INDICADORES ESTÃO PREVISTOS NO ANEXO – ESPECIFICAÇÕES MÍNIMAS OBRIGATÓRIAS.**

8.5. A dedução terá como base de cálculo os valores estipulados para a remuneração dos serviços mensais, limitados a 30% (trinta por cento) do valor daquele mês, e o resultado apurado pelo Sebrae-SP deverá corresponder ao valor da nota fiscal a ser emitida.

8.6. A adoção do ANS não impede que sejam aplicadas as penalidades previstas em contrato.

9. SUBCONTRATAÇÃO

9.1. A CONTRATADA, em nenhuma hipótese, poderá subcontratar os serviços deste objeto.

10. CRITÉRIOS DE SUSTENTABILIDADE

10.1. A CONTRATADA deverá adotar na execução do objeto contratual, práticas de sustentabilidade e de racionalização no uso de materiais e serviços, com o objetivo de atender aos critérios de redução de desperdício,

diminuição do uso intensivo de matérias primas, reciclagem, da não geração de resíduos, promover o uso consciente de recursos naturais, de modo que a prestação dos serviços seja ambientalmente responsável.

11. VIGÊNCIA

11.1. A **ata de registro de preços** terá vigência de 12 (doze) meses, podendo ser prorrogada nos termos do Regulamento de Licitações e Contratos do Sistema Sebrae.

12. GARANTIA CONTRATUAL DE EXECUÇÃO

12.1. Garantia equivalente a 5% (cinco por cento) do valor global do contrato, em uma das modalidades dentre aquelas previstas no art. 37, do Regulamento de Licitações e de Contratos do Sistema SEBRAE, a saber:

12.1.1. Caução em dinheiro.
12.1.2. Fiança bancária.
12.1.3. Seguro garantia.

12.2. A modalidade seguro-garantia somente será aceita se assegurar o pagamento de todos os eventos indicados abaixo:

12.2.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
12.2.2. Prejuízos causados ao SEBRAE-SP, decorrentes de culpa ou dolo durante a execução do contrato;
12.2.3. Multas aplicadas pelo SEBRAE-SP à CONTRATADA; e
12.2.4. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA.

12.3. A garantia ofertada deverá possuir o mesmo prazo de vigência do contrato.

12.4. Caso decorram desta avença obrigações financeiras ou acessórias após a sua conclusão (do contrato), ou caso haja renovação e seu prazo de validade expire antes da conclusão do pacto, ou ajuste de preços, deverão ser feitas as adequações necessárias quanto ao valor, vigência e cobertura da garantia prestada.

12.5. A CONTRATADA poderá optar por outra modalidade dentre àquelas previstas.

12.6. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 05 (cinco) dias úteis, contados da data em que for notificada.

12.7. Fica assegurado o direito de retenção da garantia, por parte do SEBRAE-SP, enquanto perdurarem procedimentos de aplicação de sanções contratuais.

ANEXO - ESPECIFICAÇÕES TÉCNICAS MÍNIMAS E OBRIGATÓRIAS

1. DOS REQUISITOS MÍNIMOS E OBRIGATÓRIOS

ITEM	DESCRIÇÃO	UNIDADE	QTD TOTAL PARA REGISTRO
1	Solução de Gerenciamento de Exposição Contínua a Ameaças. **Período de subscrição = 24 meses**	Unidade	1
2	Licenciamento da Capacidade de Validação de Brechas e Simulações de Ataques. **Período de subscrição = 24 meses**	Usuário	2.600
3	Licenciamento da Capacidade de Gestão de Superfície de Ataque Externo. **Período de subscrição = 24 meses**	Ativo	2.500
4	Serviço de suporte técnico especializado da solução.	Mês	24

Tabela 01 – Escopo de Fornecimento

Neste item estão especificados os requisitos mínimos e obrigatórios para todos os itens da **Tabela 01 – Escopo de Fornecimento**, onde a licitante deverá apresentar, junto a sua proposta comercial, documentação comprobatória do atendimento de todos os requisitos. A licitante deve ainda:

- Apresentar a composição de cada item do escopo de serviços, contendo marca, modelo, códigos, descritivo dos códigos, unidade, quantidades do conjunto, tudo com o objetivo de se identificar claramente os produtos e serviços ofertados.
- Apresentar documentação técnica (manuais e/ou catálogos do fabricante, em mídia eletrônica ou URL) comprovando o pleno atendimento de todos os requisitos técnicos, por meio de apresentação de uma planilha ponto a ponto, com indicação de nome do documento e página que comprova o atendimento. Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante, exceto quando explicitamente permitido.

O Sebrae/SP poderá a qualquer momento realizar diligência para comprovação da veracidade de qualquer documento apresentado. Para cada requisito técnico desse anexo, aplicar-se-á as seguintes definições.

- **Suportar**: Deve suportar a implantação da funcionalidade, de forma atual ou de forma futura via aditamento contratual.
- **Permitir**: Deve permitir e estar incluído na oferta da licitante a funcionalidade solicitada, sem custos extras ao valor ofertado pela licitante.
- **Implantar**: Deve implantar e estar incluído na oferta da licitante a funcionalidade solicitada, sem custos extras ao valor ofertado pela licitante.
- **Possuir**: Deve possuir e estar incluído na oferta da licitante a funcionalidade solicitada, sem custos extras ao valor ofertado pela licitante.
- **Fornecer**: Deve fornecer e estar incluído na oferta da licitante a funcionalidade solicitada, sem custos extras ao valor ofertado pela licitante.

1.1. Cada item da "**Tabela 01 – Escopo de Fornecimento**", deve contemplar ferramenta, ou conjunto de ferramentas, que atenda a todos os requisitos a seguir.

1.2. ITEM 01: SOLUÇÃO DE GERENCIAMENTO DE EXPOSIÇÃO CONTÍNUA A AMEAÇAS.

1.2.1. Requisitos Gerais:

1.2.1.1. Implantar plataforma base que atenda todos os requisitos técnicos desse item, através de solução de um único fabricante, ou, alternativamente, através de soluções modulares de diversos fabricantes integrados entre si.

1.2.1.2. Possuir licenciamento oficial do fabricante para os softwares e soluções ofertadas.

Não será aceito licenciamentos nas seguintes modalidades: "community (free)", “NFR (not for resale)”, “demo (demonstração)”, open source, e que não disponham de suporte e garantia oficial de atualização junto ao fabricante.

1.2.1.3. Fornecer atualizações de versões durante toda a vigência do contrato.

1.2.1.4. Possuir representante oficial do(s) fabricante(s) no Brasil.

1.2.1.5. A proposta deve apresentar nome, endereço, telefone e e-mail do representante(s) oficial (ais) no Brasil.

1.2.1.6. Implantar funcionalidades que abranja os conceitos de:

a) Validação de brechas e simulações de ataques (BAS),
b) Gestão da superfície de ataque externo (EASM), e,
c) Mecanismo de detecção de propagação de ameaças na rede.

1.2.1.7. Fornecer plataforma baseada em modelo nuvem SaaS (Software as a Service). Não serão aceitas soluções do tipo ON-premisse.

1.2.1.8. Implantar simulação, avaliação e gestão ampliada da postura de segurança da organização, medindo a eficácia por meio de testes e avaliações do nível de proteção tanto do perímetro quanto de ambientes internos, proporcionando uma visão abrangente sobre a efetividade dos controles de segurança.

1.2.1.9. Implantar capacidade ilimitada de escaneamento/simulações de ataque para as funcionalidades requisitadas neste item, bem como para as quantidades solicitadas nos ITENS 2 e 3 da Tabela 01 – Escopo de Fornecimento.

1.2.1.10. Possuir a capacidade, através de sua rede de inteligência, de fornecer informações sobre ameaças emergentes e relevantes para a plataforma, com detalhes sobre essas ameaças e as medidas de remediação recomendadas.

1.2.1.11. Permitir que profissionais de cibersegurança identifiquem, diagnostiquem, gerenciem, controlem e validem a postura de segurança cibernética de ponta a ponta.

1.2.1.12. Permitir a recriação de cenários reais de ataques à infraestrutura de segurança do SEBRAE-SP.

1.2.1.13. O volume de usuários (ITEM 2) e de Ativos (ITEM 3) para ativar as funcionalidades da plataforma base serão definidos pela contratação e demanda dos quantitativos dos ITENS 2 e 3.

1.2.1.14. Fornecer os serviços de instalação, ativação, testes da plataforma base, de forma garantir que a plataforma esteja apta a sua operação e ativação dos licenciamento dos ITENS 2 e 3 da Tabela 01 – Escopo de fornecimento.

1.2.1.15. A partir da assinatura do contrato, correrão os seguintes prazos:

1.2.1.15.1. Reunião de início do projeto (kick-off): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pelo SEBRAE com 02 (dois) dias úteis de antecedência.

1.2.1.15.2. Entrega do Projeto Executivo: até 20 (vinte) dias corridos, contados a partir da reunião de início do projeto (kick-off);

1.2.1.15.3. O SEBRAE se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;

1.2.1.15.4. Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo SEBRAE, a respeito da manifestação sobre o Projeto Executivo;

1.2.1.15.5. A conclusão da fase de implantação dos serviços é de até 60 (sessenta) dias corridos, contados a partir da data de aceite do projeto executivo, mediante a emissão do termo de recebimento definitivo pelo SEBRAE.

1.2.2. Funcionalidades Gerais:

1.2.2.1. Permitir integração com serviços de SSO, possibilitando autenticação centralizada e login seguro dos usuários na plataforma, com suporte a protocolos SAML 2.0 e OAuth 2.0, para garantir compatibilidade com os principais provedores de identidade.

1.2.2.2. Possuir compatibilidade com APIs de diversas plataformas de segurança, gerenciada por uma console central, ou alternativamente, integradas em diversos módulos, permitindo configurações, monitoramento e atualizações automáticas.

1.2.2.3. Permitir o auto provisionamento de usuários para garantia de autenticação e autorização através de grupos do AD (Active Directory). Este processo poderá ser feito via API ou interface gráfica, deste que, seja nativo do fabricante.

1.2.2.4. Permitir comunicação entre componentes via proxy web, com protocolos seguros como HTTPS e TLS 1.2 ou superiores.

1.2.2.5. Permitir a instalação de agentes de forma manual, automatizada ou em lote.

1.2.2.6. Fornecer níveis de risco após cada simulação, comparando resultados atuais e anteriores para determinar progresso ou retrocesso, e estabelecer um baseline.

1.2.2.7. Permitir a criação de regras “SIGMA” e permitir a conversão dessas regras em buscas (queries) para plataformas de “SIEM” ou criação de regras de correlação.

1.2.2.8. Permitir integrações com tecnologias de segurança, proporcionando maior visibilidade em detecção, gestão de vulnerabilidades, automação de “playbooks” e validação de processos internos.

1.2.2.9. Possuir compatibilidade com soluções de correlação de eventos “SIEM” para os produtos de segurança que não possuem integração direta.

1.2.2.10. Permitir à conversão de regras “SIGMA” para o “SIEM” da Securonix atualmente em uso na SEBRAE.

1.2.2.11. Fornecer visibilidade do status e versão dos agentes, permitindo ações como reinicialização ou desinstalação via console.

1.2.2.12. Permitir avaliar a eficácia das defesas da organização contra táticas e procedimentos de grupos criminosos conhecidos, com uma biblioteca atualizada automaticamente com ameaças emergentes.

1.2.2.13. Permitir a criação de perfis de adversários e oferecer simulações de ataques baseados nos frameworks MITRE ATTACK e TTPs disponíveis.

1.2.2.14. Possuir console de gerenciamento com dashboard que apresente informações sobre vulnerabilidades baseadas em ataques, incluindo:

1.2.2.14.1. a opção de rastreabilidade dos testes em tempo de execução.

1.2.2.14.2. interface para o gerenciamento dos ataques em andamento, visualização de logs e configurações de recursos envolvidos no ataque, incluindo proxy, e-mail, entre outros.

1.2.2.15. Permitir a geração de relatórios técnicos ou gerenciais.

1.2.2.16. Permitir a extração de dados completos em sua guia de relatórios, com informações gerais de todos os ataques realizados em um determinado vetor, além da opção de download dos relatórios em formatos PDF, CSV ou TXT.

1.2.2.17. Permitir a geração e download de relatórios via interface e permitir o envio por e-mail.

1.2.2.18. Implantar a geração de relatórios e uma visão detalhada segmentada por ambientes.

1.2.2.19. Implantar uma visão clara do desempenho individual de cada vetor de ataque, incluindo um gráfico de comparação para benchmark.

1.2.2.20. Fornecer um caminho simplificado para, no mínimo:

1.2.2.20.1. Abrir chamados.

1.2.2.20.2. Gerenciar usuários da plataforma.

1.2.2.20.3. Acessar documentações do produto.

1.2.2.20.4. Gerenciar logs e atividades em execução.

1.2.3. Funcionalidades de Validação de Brechas e Simulações de Ataques (BAS):

1.2.3.1. Implantar simulações automáticas, voltadas para a avaliação de ajustes e configurações de diferentes controles de segurança.

1.2.3.2. Implantar validação de controles de segurança, para no mínimo, as seguintes ferramentas de proteção:

1.2.3.2.1. Soluções de Proteção de Endpoints (Endpoint Protection/EDR) .

1.2.3.2.2. Gateway de E-mail Seguro (Mail Gateway Security).
1.2.3.2.3. Gateway de Web Seguro (Secure Web Gateway).
1.2.3.2.4. Firewall de Aplicação Web Seguro (Web Application Firewall).
1.2.3.2.5. DLP (Data Loss Prevention).

1.2.3.3. Implantar simulações de ataque através de um agente único ao qual deverá ser capaz de executar ataques em diferentes vetores de forma individual ou simultânea.

1.2.3.4. Permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma isolada, além de possibilitar simulações que respeitem o ciclo de vida completo de um ataque.

1.2.3.5. Permitir identificar quais testes foram bem-sucedidos e quais falharam durante o processo de prevenção. Para os resultados, deve ser possível gerar evidências de detecção e/ou bloqueio através de integração com um SIEM e/ou diretamente no dispositivo que detectou e/ou bloqueou a simulação.

1.2.3.6. Implantar as simulações a partir de componentes da solução ou de um equipamento dedicado exclusivamente a simulação.

1.2.3.7. Permitir que ao concluir ataques, seja com vetores de ataque individualmente ou em conjunto, apresentar um score de risco com uma visão clara da maturidade atual e histórica do ambiente.

1.2.3.8. Permitir para a validação do vetor de endpoint, simulações de ataque para:

1.2.3.8.1. Ransomware: Avaliação da eficácia dos recursos para detecção de comportamentos anômalos durante a execução segura de ransomwares, que devem buscar arquivos sensíveis no host e usar chaves geradas de forma controlada para criptografia de arquivos.

1.2.3.8.2. Worm: Avaliação da eficácia dos recursos para detecção de comportamentos anômalos durante a execução segura de worms, que devem realizar a descoberta de hosts vulneráveis e simular a proliferação por meio de protocolos, como SMB.

1.2.3.8.3. Trojan: Avaliação da eficácia dos recursos para detecção de comportamentos anômalos durante a execução segura de trojans, com coleta de informações do host, como nome de usuário e e-mail, além da possibilidade de estabelecer comunicação usando métodos diversos de reverse shell.

1.2.3.8.4. Antivírus: Avaliação da eficácia de inspeção e proteção contra ameaças de arquivos maliciosos, com malwares em disco sendo atualizados diariamente por meio de múltiplos feeds de segurança.

1.2.3.8.5. MITRE ATT&CK: Avaliação da eficácia dos recursos anti-malware com comandos customizados que simulam o comportamento de adversários conforme o framework ATT&CK.

1.2.3.9. Permitir para validação do vetor de e-mail gateway, simulações de ataque para:

1.2.3.9.1. Ransomware: Avaliação dos recursos de proteção de e-mail com técnicas de execução de ransomwares, em execução segura.

Worm: Avaliação dos recursos de proteção de e-mail com técnicas de execução de worms, de forma segura.

1.2.3.9.2. Malware: Avaliação de proteção de e-mail com execução de malwares, simulando cenários interativos, como UAC, roubo de credenciais e C&C.

1.2.3.9.3. Payload: Avaliação dos recursos de proteção de e-mail com técnicas de execução de payloads em ambiente seguro.

1.2.3.9.4. Exploits: Avaliação dos recursos de proteção de e-mail com execução de arquivos que exploram vulnerabilidades em programas.

1.2.3.9.5. Dummy: Avaliação dos recursos de proteção de e-mail utilizando payloads conhecidos, como MessageBox do Metasploit, em ambiente seguro.

1.2.3.9.6. True File Type Detection: Avaliação da proteção de e-mail com envio de arquivos cuja extensão difere do formato original, para identificar possíveis brechas.

1.2.3.10. Permitir para validação do vetor de web application firewall (WAF), simulações de ataque para:

1.2.3.10.1. SQL Injection.
1.2.3.10.2. Cross-site Scripting (XSS).
1.2.3.10.3. NoSQL Injection.
1.2.3.10.4. XML Injection.
1.2.3.10.5. Path Traversal.
1.2.3.10.6. Inclusão de Arquivo para Execução Remota de Código.
1.2.3.10.7. Injeção de Comando.
1.2.3.10.8. WAF Bypass.

1.2.3.11. Permitir para validação de vazamento de dados (DLP), simulações de ataque para os métodos abaixo:

1.2.3.11.1. HTTP & HTTPS: Exfiltração de dados por HTTP/S, injetando dados confidenciais nos cabeçalhos de solicitação enviados a um servidor remoto.
1.2.3.11.2. Navegadores HTTP & HTTPS: Exfiltração de dados via navegadores como IE, Edge e/ou Chrome.
1.2.3.11.3. DNS: Exfiltração de dados pela porta 53.
1.2.3.11.4. Tunelamento DNS: Exfiltração via protocolo DNS, com injeção de dados em solicitações DNS.
1.2.3.11.5. Tunelamento ICMP: Exfiltração usando cabeçalhos ICMP com pacotes ECHO para um servidor remoto.
1.2.3.11.6. Telnet: Exfiltração pela porta 23 do Telnet.
1.2.3.11.7. SFTP: Exfiltração pelo protocolo SFTP.
1.2.3.11.8. Outras Portas: Exfiltração via upload de dados para servidores externos por portas abertas.
1.2.3.11.9. Email: Exfiltração usando e-mail corporativo no Outlook.
1.2.3.11.10. Serviços de Nuvem: Exfiltração para ou através de aplicativos e serviços em nuvem.
1.2.3.11.11. Dispositivos Removíveis: Exfiltração via cópia para dispositivos removíveis, como USB.

1.2.4. Funcionalidades de Detecção de Propagação de Ameaças na Rede:

1.2.4.1. Implantar recursos para avaliar o impacto de políticas de segmentação de rede e a eficácia de controles internos contra a movimentação lateral.

1.2.4.2. Possuir a capacidade de simular movimentos de ataque em tempo real, visando identificar e explorar pontos de fragilidade que permitam o movimento não autorizado entre segmentos da rede.

1.2.4.3. Permitir simulações de ataque para a verificação dos seguintes métodos:

1.2.4.3.1. Pass-the-Password.
1.2.4.3.2. Pass-the-Ticket.
1.2.4.3.3. Pass-the-Hash.
1.2.4.3.4. Brute Force.
1.2.4.3.5. LLMNR/NBT-NS Poisoning and Relay.
1.2.4.3.6. Kerberoast.
1.2.4.3.7. Password Spraying.
1.2.4.3.8. Roubo de senhas LAPS.
1.2.4.4. Permitir a criação de modelos personalizados nos vetores de ataque, sem impactar o ambiente.

1.2.4.5. Possuir recursos para configurar e adaptar o comportamento de testes para simular diferentes vetores de ataque, permitindo uma avaliação detalhada da resposta do ambiente a movimentações laterais

1.2.4.6. Permitir que o agente da solução atue de forma idêntica a um atacante real, sem necessidade de outros agentes para validar diferentes métodos.

1.2.4.7. Permitir o “pivoting” na rede, fornecendo um mapa completo da trilha percorrida e dos alvos alcançados, permitindo a identificação de alvos que podem ser considerados joias da coroa (Crown Jewels) ou não.

1.2.5. Funcionalidades de Gerenciamento de Superfície de Ataque Externo:

1.2.5.1. Permitir identificar automaticamente ativos externos da organização, como domínios, subdomínios, IPs, servidores expostos e outras interfaces públicas, que possam ser alvos de ataques.

1.2.5.2. Implantar varreduras contínuas para detectar novos ativos e mudanças no ambiente externo da organização, proporcionando visibilidade em tempo real das possíveis vulnerabilidades e riscos.

1.2.5.3. Permitir classificar e priorizar as vulnerabilidades descobertas com base no risco que representam para a organização, levando em conta o impacto e a criticidade dos ativos.

1.2.5.4. Permitir monitorar a internet e a dark web em busca de possíveis vazamentos de dados sensíveis da organização, como credenciais comprometidas ou outras informações críticas.

1.2.5.5. Permitir a consolidação das informações de ativos, vulnerabilidades e riscos em um painel unificado, facilitando a gestão e resposta aos problemas identificados.

1.2.5.6. Permitir a automação de alertas e a geração de relatórios personalizados, notificando os responsáveis pelas áreas de segurança sobre novos riscos ou vulnerabilidades descobertas.

1.2.5.7. Permitir simular ataques externos contra a organização para avaliar a eficácia dos controles de segurança e identificar pontos fracos na defesa.

1.2.5.8. **Entregável:**

1.2.5.8.1. Apresentar evidências da ativação da plataforma no formato SaaS.

1.2.5.8.2. Relatório as-built da ativação da plataforma em nome do SEBRAE.

1.3. ITEM 02: LICENCIAMENTO DA CAPACIDADE DE VALIDAÇÃO DE BRECHAS E SIMULAÇÕES DE ATAQUES.

1.3.1. Métrica: Cada “usuário” ou “agente” representa 1 (um) unidade de licenciamento desse item.

1.3.1.1. Permitir que o licenciamento seja dimensionado conforme o número de usuários ou agentes nos quais a simulação de segurança será aplicada, visando cobrir áreas críticas da infraestrutura organizacional.

1.3.2. Permitir a realização de simulações ilimitadas e automatizadas de ataques cibernéticos no ambiente do SEBRAE para o número de usuários definidos no escopo de fornecimento.

1.3.2.1. O licenciamento desse item ativa as funcionalidades de software das seções “Funcionalidades de Validação de Brechas e Simulações de Ataques (BAS)” e “Funcionalidades de Detecção de Propagação de Ameaças na Rede” do ITEM 01 da Tabela 1 – Escopo de fornecimento.

1.3.3. **Entregável:**

1.3.3.1. Relatório as-built com evidências da ativação na plataforma do ITEM 01 do volume de licenças adquiridas através do ITEM 02.

1.4. ITEM 03: LICENCIAMENTO DA CAPACIDADE DE GESTÃO DE SUPERFÍCIE DE ATAQUE EXTERNO.

1.4.1. Métrica: Cada “ativo” ou “asset” representa 1 (um) unidade de licenciamento desse item.

1.4.1.1. Permitir que o licenciamento seja baseado na quantidade de ativos monitorados, sendo que cada ativo se refere a um componente digital externo (ex.: subdomínios, endereços IP públicos IPV4 e IPV6, ASN, e-mails, web services, aplicativos web) que compõe a superfície de ataque exposta.

1.4.1.2. Permitir o monitoramento dos ativos digitais expostos encontrados pelo módulo de Gestão de Superfície de Ataque Externo, garantindo a segurança e a continuidade operacional da organização.

1.4.1.3. O licenciamento desse item ativa as funcionalidades de software da seção “Funcionalidades de Gerenciamento de Superfície de Ataque Externo” do ITEM 01 da Tabela 1 – Escopo de fornecimento.

1.4.1.4. **Entregável:**

1.4.1.4.1. Relatório as-built com evidências da ativação na plataforma do ITEM 01 do volume de licenças adquiridas através do ITEM 03.

1.5. ITEM 04: SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO DA SOLUÇÃO.

1.5.1. O serviço de suporte técnico especializado para a solução deve prever assistência técnica contínua e personalizada, garantindo que o SEBRAE maximize o valor da solução contratada.

1.5.2. O serviço deve possuir alinhamento ao programa de **Gerenciamento Contínuo de Ameaças (CTEM)** do Gartner, contemplando as seguintes etapas: definição do escopo, descoberta, priorização, validação e mobilização.

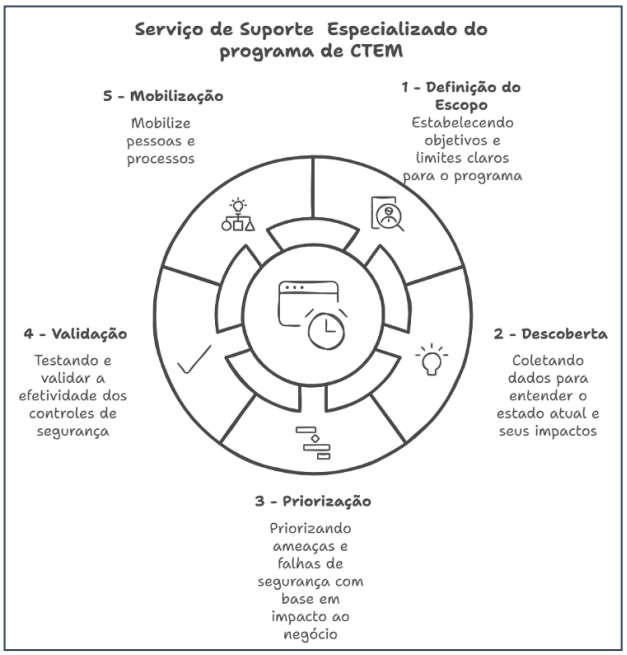


Figura 1 - Etapas do Serviço de Suporte Especializado

1.5.3. As atividades de suporte técnico especializado do programa de CTEM a serem realizadas pela CONTRATADA devem contemplar os seguintes objetivos e atividades:

1.5.4. Definição do Escopo

1.5.4.1. Objetivo

1.5.4.1.1. Definir claramente os objetivos do programa de CTEM e o resultado desejado, alinhando-os com a visão estratégica do SEBRAE. Esta fase é crucial para que o processo de CTEM a ameaças seja direcionado e focado, permitindo uma proteção eficaz dos ativos mais críticos.

1.5.4.2. Atividades

1.5.4.2.1. Implantar uma definição do escopo de atuação da solução de CTEM.

1.5.4.2.2. Implantar a coleta de informações de contato dos usuários, equipes técnicas e de segurança para garantir uma integração eficiente.

1.5.4.2.3. Implantar o estabelecimento de KPIs para acompanhar a evolução da solução.

1.5.4.3. Descoberta

1.5.4.3.1. Objetivo

1.5.4.3.1.1. Coletar dados e informações para entender o estado atual de exposição à riscos cibernéticos e seus impactos no SEBRAE. Esta fase busca criar um inventário abrangente dos ativos, serviços, sistemas e suas potenciais falhas de segurança, formando a base para as fases subsequentes de priorização e mobilização.

1.5.4.3.2. Atividades

1.5.4.3.2.1. Implantar o mapeamento de ativos visando identificar os ativos críticos, incluindo sistemas, redes, dispositivos e aplicações.

1.5.4.3.2.2. Implantar a avaliação das áreas de exposição que podem ser exploradas por atacantes, como interfaces externas e serviços acessíveis pela internet.

1.5.4.3.2.3. Implantar o mapeamento de possíveis caminhos de ataque.

1.5.4.3.2.4. Implantar a identificação de vulnerabilidades e exposições descobertas para que possam ser priorizadas e tratadas nas próximas fases.

1.5.4.4. Priorização

1.5.4.4.1. Objetivo

1.5.4.4.1.1. Priorizar as ameaças e falhas de segurança mais críticas de acordo com a criticidade e o impacto potencial que representam para o SEBRAE. Esta fase é essencial para que a equipe de segurança possa concentrar esforços nas ameaças que oferecem maior risco, otimizando o uso de recursos para reduzir a superfície de ataque de forma eficiente.

1.5.4.4.2. Atividades

1.5.4.4.2.1. Implantar análise das ameaças para entender como as vulnerabilidades podem impactar o SEBRAE.

1.5.4.4.2.2. Implantar avaliação do impacto potencial de cada ameaça ou vulnerabilidade nos ativos críticos.

1.5.4.4.2.3. Implantar, em conjunto com o SEBRAE, um nível aceitável de risco de segurança e revisá-lo periodicamente para garantir que esteja dentro dos limites estabelecidos.

1.5.4.4.2.4. Fornecer um plano preliminar de mitigação com foco nas ameaças e vulnerabilidades mais críticas.

1.5.4.5. Validação

1.5.4.5.1. Objetivo

1.5.4.5.1.1. Testar e validar a efetividade dos controles de segurança. Esta fase envolve a validação das suposições sobre vulnerabilidades e o cenário de ameaças feitas nas três fases anteriores. Confirma vulnerabilidades, vetores de ataque e a eficácia da estratégia de resposta a incidentes.

1.5.4.5.2. Atividades

1.5.4.5.2.1. Implantar testes de simulação de ataque visando a validação dos controles de segurança vigentes.

1.5.4.5.2.2. Implantar avaliação da probabilidade de sucesso de um ataque validando se os invasores conseguem realmente explorar os pontos fracos identificados, separando problemas críticos de falsos positivos.
Implantar avaliação do plano de resposta a incidentes para validar se os atuais controles de segurança e procedimentos de resposta a incidentes da organização são suficientes para impedir ataques reais direcionados a esses pontos fracos.

1.5.4.6. Mobilização

1.5.4.6.1. Objetivo

1.5.4.6.1.1. Mobilizar a equipe técnica do SEBRAE para a garantir que as equipes operacionalizem as remediações por meio de ações claras. Esta fase envolve garantir que os usuários, ferramentas e processos estejam alinhados e prontos para enfrentar as ameaças identificadas de maneira proativa e coordenada.

1.5.4.6.2. Atividades

1.5.4.6.2.1. Implantar reuniões periódicas (minimamente mensais) com a equipe técnica do SEBRAE para avaliar o progresso e fornecer recomendações para melhorar a postura de segurança.

1.5.4.6.2.2. Implantar revisões estratégicas periódicas (minimamente trimestrais) consolidadas, apresentando relatórios executivos e resultados detalhados das avaliações realizadas.

1.5.4.6.2.3. Fornecer apoio na análise de dados e resultados das avaliações, de forma a extrair percepções estratégicas para a tomada de decisões de segurança.

1.5.4.6.2.4. Fornecer relatórios executivos periódicas (minimamente trimestrais), detalhando os resultados e oferecendo percepções para a melhoria contínua da segurança cibernética.

1.5.4.7. O serviço deverá ainda:

1.5.4.7.1. Fornecer desde a reinstalação e configuração da solução até a resolução de problemas e otimização de processos, permitindo a manutenção de uma postura proativa contra ameaças cibernéticas.

1.5.4.7.2. Implantar métodos para configurar permissões de usuário e notificações de acordo com o licenciamento.

1.5.4.7.3. Fornecer assistência na instalação de agentes e resolução de possíveis problemas da plataforma.

1.5.4.7.4. Fornecer repasse de conhecimento semestral, com carga horária mínima de 8 horas, para até 4 profissionais do SEBRAE, cobrindo configurações e gerenciamento da solução.

1.5.4.7.5. Implantar métodos de revisão e refinamento do uso da plataforma, de forma a alinhar as práticas do SEBRAE com as melhores práticas de mitigação de riscos.

1.5.4.7.6. Implantar métodos que garantam que as notificações e alertas da plataforma sejam configuradas para apenas os usuários autorizados.

1.5.4.7.7. Fornecer documentação detalhada, do tipo As-Built, para apoiar o SEBRAE na avaliação do funcionamento da solução.

1.5.4.7.8. Fornecer suporte remoto contínuo, ou on-site quando necessário, para permitir que o SEBRAE resolva dúvidas ou problemas de uso.

1.5.4.7.9. Implantar métodos para garantir que todos os usuários administradores da plataforma estejam cientes das permissões e responsabilidades dentro do sistema, minimizando erros operacionais.

1.5.4.7.10. Implantar serviço de painéis (dashboards) executivos, com indicadores de performance, segurança, operação e administração da solução, de forma que permita o SEBRAE monitorar a execução dos serviços prestados.

1.5.4.8. **Deverá ainda:**

1.5.4.8.1. Implantar o serviço no formato SaaS em nuvem.

1.5.4.8.2. É de responsabilidade da CONTRATADA a definição, criação e manutenção dos indicadores e painéis, de forma que o SEBRAE possa consumir os painéis prontos.

1.5.4.8.3. Permitir acesso através de interface Web (HTTPS), com controle de acesso por identificação de usuário e solicitação de senha e duplo fator de autenticação, ambos de forma individual por usuário através de Software Token (“tokens baseados em software”).

1.5.4.8.4. Possuir recurso de “reset” de senha, de forma que que o usuário receba por e-mail, link para reset da senha ou nova senha temporária de acesso.

1.5.4.8.5. Permitir o cadastramento de no mínimo 05 (usuários) do SEBRAE para visualização dos painéis disponibilizados.

1.5.4.8.6. Possuir tecnologia do tipo responsiva, de forma que a visualização se adapte ao tamanho da tela dos dispositivos utilizados no acesso.

1.5.4.8.7. Implantar controle de acesso por usuário, de forma a controlar o grupo de assunto ou painel que pode ser visualizado.

1.5.4.8.8. Possuir a capacidade de coleta de dados de forma agendada, recorrente e automática.

1.5.4.8.9. Permitir a visualização gráfica de indicadores por tabelas, KPIs, gráficos, texto formatados, através de:

1.5.4.8.9.1. Caixas de Textos, permitindo a inclusão de imagens, HTML e formatações de fonte, borda e cores.

1.5.4.8.9.2. KPIs (key performance indicators).

1.5.4.8.9.3. Tabelas (Linha x Coluna).

1.5.4.8.9.4. Gráficos, com diversos tipos de gráficos (pizza, barras, linha, dispersão, bolha, área).

1.5.4.8.10. Permitir filtro interno e individualizado por painel, através de:

1.5.4.8.10.1. um ou mais campos de dados.

1.5.4.8.10.2. valores individuais a cada campo incluído no filtro.

1.5.4.8.10.3. intervalos do tipo acima de, abaixo de, entre valor inicial e final.

1.5.4.8.10.4. Top N e Down N.

1.5.4.8.10.5. contagem normal e distinta.

1.5.4.8.10.6. soma, valor máximo, valor mínimo, média, mediana e valor real.

1.5.4.8.10.7. data através dos critérios de filtro por ano, trimestre, mês, dia, semana, dia da semana, dia do mês, data real, data e hora real, hora e intervalos entre datas.

1.5.4.8.11. Permitir a seleção de filtros relacionados ao indicador ou ao painel através de campos diversos. A seleção deve ser realizada em caixa de seleção individual ou de múltiplos valores para cada filtro.

1.5.4.8.12. Permitir a exportação de indicadores gráficos no formato de imagem ou pdf.

1.5.4.8.13. Permitir a definição de senha para posterior acesso ao arquivo exportado.

1.5.4.8.14. A LICITANTE deve informar a plataforma a ser utilizada, bem como apresentar comprovação do atendimento dos requisitos.

1.5.4.9. Implantar todos **os** requisitos descritos no ITEM 2- DOS REQUISITOS MÍNIMOS E OBRIGATÓRIOS DOS SERVIÇOS DE GARANTIA E SUPORTE.

1.5.4.10. **Entregável**:

1.5.4.10.1.1. Relatórios periódicos, minimamente mensais e trimestrais, com o detalhamento dos serviços executados.

2. DOS REQUISITOS MÍNIMOS E OBRIGATÓRIOS DOS SERVIÇOS DE GARANTIA E SUPORTE

Os serviços de garantia e suporte devem ser prestados pela CONTRATADA, nos seguintes termos.

Entende-se por “Garantia” ou “Suporte” ou “Manutenção”, doravante denominada unicamente como “Garantia”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de prestação de serviços. Esta possui suas causas em falhas e erros no Software/Hardware e trata da correção dos

problemas atuais e não iminentes. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços, tais como:

Do hardware: quando aplicável, incluir à desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.

Do software: quando aplicável, incluir à desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados.

Quanto às atualizações pertinentes aos softwares: Entende-se como “atualização” o provimento de toda e qualquer evolução de software, oficial e comprovadamente disponibilizada pelo fabricante da solução, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a necessidade de atualização de tais versões ocorra durante o período contratado.

A CONTRATADA aplicará pacotes de correção oficiais do fabricante, em data e horário a serem definidos pelo SEBRAE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato.

O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software, independente da severidade do chamado.

É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de “Garantia” do tipo “Preventiva” que pela sua natureza reduza a incidência de problemas que possam gerar “Garantia” do tipo “Corretiva”.

A manutenção técnica do tipo “corretiva” será realizada sempre que solicitada pelo SEBRAE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA via telefone (com número do tipo “0800” caso a Central de Atendimento esteja fora de São Paulo - SP) ou Internet ou e-mail ou outra forma de contato.

Os serviços de “Garantia” incluem:

Solução de problemas relativos à indisponibilidade da solução.

Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros.
Esclarecimento de dúvidas sobre a prestação dos serviços.

Instalação de novas versões ou atualizações e patches. Esse serviço deverá ser realizado em horário a ser definido pelo SEBRAE.

A CONTRATADA deve disponibilizar a central atendimento 24 horas por dia, 7 dias da semana e equipe com conhecimentos sólidos no serviço prestado.

O serviço de “Garantia” deve disponibilizar os seguintes tipos de atendimento:

Nível I - Atendimento Telefônico (Help Desk): chamados abertos através de ligação telefônica ou e-mail ou outra forma de contato, em regime de 24x7: 24 horas por dia, 7 dias da semana. Esse serviço deve atender demandas dos usuários referentes ao serviço prestado.

Nível II - Atendimento Remoto: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pelo SEBRAE, mediante prévia autorização e seguindo os padrões de segurança do SEBRAE, objetivando análise e solução remota dos problemas apresentados.

Nível III - Atendimento Presencial (On-Site): quando aplicável, os atendimentos técnicos realizados nas dependências do SEBRAE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto.

Toda "Garantia" deve ser solicitada inicialmente via Help Desk (Nível I), ficando a transferência do atendimento para o Atendimento Remoto (Nível II) condicionado à autorização do SEBRAE.
Toda "Garantia" solicitada inicialmente via Help Desk (Nível I), deve ser transferido para o Atendimento Presencial (Nível III) quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte Acordo de Níveis de Serviços (ANS) e sua SEVERIDADE:

SEVERIDADE URGENTE – Solução totalmente inoperante.

Prazo máximo de início de atendimento de até 01 hora úteis contadas a partir do horário de abertura do chamado.

Prazo máximo de resolução do problema de até 12 horas úteis contadas a partir do início do atendimento.

SEVERIDADE IMPORTANTE – Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.

Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado.

Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.

SEVERIDADE NORMAL – Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.

Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado.

Prazo máximo de resolução do problema de até 48 horas úteis contadas a partir do início do atendimento.

SEVERIDADE EXTERNO – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não disponibilizado pela CONTRATADA.

Neste caso, ficam suspensos todos os prazos de atendimento até que o SEBRAE resolva os problemas externos que provocam a inoperância da solução. Após o SEBRAE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.

SEVERIDADE INFORMAÇÃO – Solicitações de informações diversas ou dúvidas sobre a solução.
Prazo máximo de resposta de até 2 dias úteis, contados a partir da data de abertura da ocorrência.
Um chamado técnico somente poderá ser fechado após a confirmação do responsável do SEBRAE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde está instalado.

Na abertura de chamados técnicos, será informado pelo SEBRAE a severidade do chamado.
A severidade do chamado poderá ser reavaliada pelo SEBRAE, quando verificado que foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.

A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

A quantidade de chamados atendidos será agrupada em dois índices, calculados separadamente, conforme abaixo:

Indicador de Início de Atendimento (IIA): Mostra o nível de cumprimento do prazo previsto para início de atendimento dos chamados de Atendimento. Deve ser apurado separadamente, por linha de serviço, conforme serviços que estejam em uso pelo SEBRAE:

<table>
<tr><th colspan="3">Indicador IIA</th></tr>
<tr><td>1</td><td>Periodicidade</td><td>A apuração deve ser medida considerando os chamados do SEBRAE concluídos entre o primeiro e o último dia de cada mês.</td></tr>
<tr><td>2</td><td>Método de Medição (Fórmula)</td><td>IIA = (∑ quantidade de chamados de Atendimento concluídos que atenderam o ANS Início de atendimento) / (total de chamados de Atendimento concluídos no período).</td></tr>
<tr><td>3</td><td>Desconto</td><td>O percentual de desconto IIA será aplicado, sobre cada índice obtido, seguindo a tabela abaixo:
<table>
<tr><th>% Índice IIA</th><th>Percentual de De desconto do Valor Mensal</th></tr>
<tr><td>95% a 100%</td><td>0%</td></tr>
<tr><td>80% a 94,99%</td><td>2%</td></tr>
<tr><td>Abaixo de 80%</td><td>5%</td></tr>
</table></td></tr>
<tr><td>4</td><td>Cálculo de desconto</td><td>Valor de desconto (R$) = (% de desconto IIA) x (Valor total do serviço a ser pago no mês de apuração).</td></tr>
</table>

Indicador de Tempo de Solução de Atendimento (ITSA): Mostra o nível de cumprimento dos prazos previstos para tempo de solução dos chamados de Atendimento. Deve ser apurado separadamente, por linha de serviço, conforme serviços que estejam em uso pelo SEBRAE:

Indicador ITSAE		
1	Periodicidade	A apuração deve ser medida considerando os chamados de Atendimento do SEBRAE concluídos entre o primeiro e o último dia de cada mês.
2	Método de Medição (Fórmula)	ITSA = (∑ quantidade de chamados de Atendimento concluídos que atenderam o ANS tempo de solução) / (total de chamados de Atendimento concluídos no período).

<table>
<tr><td>3</td><td>Desconto</td><td>O percentual de desconto ITSA será aplicado, sobre cada índice obtido, seguindo a tabela abaixo:<table><tr><th>% Índice ITSA</th><th>Percentual de Desconto</th></tr><tr><td>95% a 100%</td><td>0%</td></tr><tr><td>80% a 94,99%</td><td>2%</td></tr><tr><td>Abaixo de 80%</td><td>5%</td></tr></table></td></tr>
<tr><td>4</td><td>Cálculo da Desconto</td><td>Valor de desconto (R$) = (%desconto ITSA) x (Valor total do serviço a ser pago no mês de apuração)</td></tr>
</table>

No mês de apuração, a soma dos valores de desconto dos indicadores IIA e ITSA será descontada do valor devido pela prestação de serviços, limitado a 10%.

Os primeiros 90 (noventa) dias a partir da primeira entrega serão considerados como período de estabilização e de ajustes específicos. Durante esse período, o ANS poderão ser flexibilizados por concordância entre as partes.

A partir do 91º (nonagésimo primeiro) a partir da primeira entrega, todo o passivo de problemas evidenciado deverá estar solucionado, cabendo a aplicação do nível de serviço sobre o passivo não solucionado e cuja responsabilidade seja exclusivamente da CONTRATADA.

A cada 3 meses, os ANS poderão ser revistos em comum acordo entre as partes, baseado nos indicadores de atendimento. Esse acordo será firmado mediante nota técnica emitida pela UTIC e respectiva carta de resposta com a concordância da CONTRATADA.

Dentro do prazo máximo de início de atendimento, cabe a CONTRATADA acionar o FABRICANTE para execução das providências que serão adotadas para a solução do chamado.

A interrupção dos serviços de atendimento para chamados de severidades 1 e 2 é vedada até o completo restabelecimento de todas as funções do sistema indisponível.

Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependam de:

Correção de falhas (bugs) pelo Fabricante.
Liberação de novas versões e patches de correção da solução pelo Fabricante.
Correção de falhas na infraestrutura de TI de responsabilidade do SEBRAE.
Correção de falhas de integração da solução com produtos de terceiros não fornecidos pela CONTRATADA.

LAYER

Conecte o presente,

proteja o futuro.

Proposta Comercial

Registro de Preços para contratação de empresa para o fornecimento de Solução de Gerenciamento de Exposição Contínua a Ameaças Cibernéticas, com serviços de implantação, suporte técnico e repasse de conhecimento, para atendimento as demandas do SEBRAE-SP.

Pregão Eletrônico N° 90051/2025 (SRP)

SHN Quadra 1 - Bloco A - Salas 708/709 – Ed. Le Quartier - Asa Norte
Brasília – DF - 70.701-010
(61) 3544-7273
www.layer.net.br

Brasília, 15 de agosto de 2025.

Prezado(a),
SERVIÇO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS DO ESTADO DE SÃO PAULO – SEBRAE-SP.

Aos cuidados da **Coordenação de Licitações e Contratos.**
Rua Vergueiro, 1.117, Paraíso,
CEP: 01.504-001, São Paulo/SP

PROPOSTA DE PREÇOS – AJUSTADA AOS LANCES

Referência: **PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOES Nº 90051/2025**
Processo: 0084/2025

LAYER TECNOLOGIA DA INFORMAÇÃO LTDA, inscrita no CNPJ nº 04.929.322/0001-70 e inscrição estadual nº 07.632.255/001-78, estabelecida na SHN QUADRA 1 CONJUNTO A BLOCO A ENTRADA A, SALAS 708/709, Asa Norte, Cep 70.701-010 – Brasília/DF, apresenta, proposta comercial para Registro de Preços para contratação de empresa para o fornecimento de ***solução de gerenciamento de exposição contínua a ameaças cibernéticas, com serviços de implantação, suporte técnico e repasse de conhecimento, para atendimento as demandas do SEBRAE-SP***, cujas especificações constam do termo de referência.

Atenciosamente,

VICTOR ARAUJO FREIRE:53341082115

Digitally signed by VICTOR ARAUJO FREIRE:53341082115
Date: 2025.08.15 16:50:47 -03'00'

VICTOR ARAUJO FREIRE
Responsável Legal

LAYER TECNOLOGIA DA INFORMAÇÃO LTDA

1 Sobre a Layer

Na Layer acreditamos que a chave para o sucesso no ambiente digital está em **conectar o presente e proteger o futuro**. Oferecemos soluções avançadas em infraestrutura de dados e cibersegurança que permitem às empresas não apenas otimizar sua operação no agora, mas também se proteger contra os desafios e ameaças do amanhã.

Nossa expertise em **infraestrutura de dados** garante que sua empresa tenha uma base sólida e escalável, capaz de armazenar, processar e gerenciar grandes volumes de informações com eficiência. Ao integrar essa infraestrutura com soluções de **cibersegurança** de ponta, oferecemos uma proteção contínua contra as ameaças digitais, assegurando a confidencialidade, integridade e disponibilidade dos dados.

Combinando inovação, tecnologia de ponta e conhecimento especializado, nossa missão é fornecer um ambiente seguro, resiliente e preparado para o futuro, permitindo que nossos clientes se concentrem no crescimento do seu negócio com total confiança na sua infraestrutura de dados.

2 Programa de Integridade

O programa de integridade Layer, é uma iniciativa que busca promover uma cultura de ética, transparência e conformidade nas operações da empresa. Ele envolve a implementação de políticas e procedimentos que visam prevenir e detectar comportamentos ilegais, antiéticos e fraudes, tanto por parte dos colaboradores quanto dos fornecedores e parceiros de negócios.

Além disso, nosso programa de integridade contempla a realização periódica de treinamentos, bem como contemplou a criação de canais de denúncia e a realização de auditorias regulares para garantir que as políticas estão sendo seguidas e a cultura de integridade está sendo mantida. A implementação do programa de integridade trouxe diversos benefícios para a empresa, como o fortalecimento da reputação, a redução de riscos legais e a melhoria do desempenho financeiro. Nosso programa de integridade está disponível em https://layer.net.br/wp-content/uploads/2023/10/Layer_Programa-de-Integridade-.pdf.

A Layer conquistou ainda em 2021 o selo CertiGov
. O selo ajuda a manter o fomento de uma cultura ética de anticorrupção e antissuborno na empresa, fornecedores e parceiros, de forma que tenham o mesmo rigor com padrões éticos e normas anticorrupção em que se baseiam. O selo trouxe os seguintes benefícios a empresa:

- Fortalecimento da cultura e práticas de antissuborno e anticorrupção por toda a empresa.
- Redução do risco do envolvimento em situações ilícitas e fraudulentas.
- Melhoria da governança empresarial.
- Aumento da credibilidade junto a clientes do setor público e privado.
- Manutenção da prática de compliance de forma preventiva e não reativa.
- Garantia de eficiência e aumento de segurança nas práticas de vendas para o mercado.

3 Proposta de Preços

ITEM	DESCRIÇÃO	PAGAMENTO	UNIDADE	QTD.	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de gerenciamento de Exposição Continua a Ameaças. **Período de subscrição = 24 meses**	Parcelas Anuais	Unidade	1	798.000,00	798.000,00
2	Licenciamento da Capacidade de validação de Brechas e Simulações de Ataques. **Período de subscrição: 24 meses**	Parcelas Anuais	Usuário	2.600	280,00	728.000,00
3	Licenciamento da Capacidade de Gestão de Superfície de Ataque Externo. **Período de subscrição: 24 meses**	Parcelas Anuais	Ativo	2.500	227,00	567.500,00
4	Serviço de suporte técnico especializado da solução	Mensal	Mês	24	9.000,00	216.000,00
					Valor Total	**2.309.500,00**

3.1 Valor Total da Proposta: **R$ 2.309.500,00** (Dois milhões, trezentos e nove mil e quinhentos reais).

3.2 A proposta é válida por 90 (noventa) dias, a contar da data de sua apresentação.

3.3 O detalhamento da marca, modelo, versão e demais características dos produtos e serviços ofertados constam da **Seção Caderno Técnico**.

4 Dados da Empresa

Dados da empresa		
Razão Social: LAYER TECNOLOGIA DA INFORMAÇÃO LTDA		
CNPJ: 04.929.322/0001-70	Inscrição Estadual nº: 07.632.255/001-78	
Endereço: SHN QUADRA 1 CONJUNTO A BLOCO A ENTRADA A, SALAS 708/709, Asa Norte		
Telefone: (61) 3544-7273	Fax: (61) 3544-7273	
E-mail: comercial@layer.net.br	Cidade/UF: Brasília/DF	Cep: 70.701.010
Representantes legais com poderes para assinar o contrato CONJUNTAMENTE		
Nome	Cargo	e-mail
Rodrigo Garcia Medeiros	Diretor Comercial	comercial@layer.net.br
Victor Araújo Freire	Diretor Executivo	comercial@layer.net.br
Dados Para Suporte		
Telefone: 61-3544-7273	e-mail: suporte@layer.net.br	site suporte: https://layer.movidesk.com/

5 Declarações

Layer Tecnologia da Informação Ltda, através dos seus representantes legais, declara para os devidos fins que se aplicam a presente proposta que:

5.1 inexistem fatos impeditivos para sua habilitação no certame ou de sua contratação, ciente da obrigatoriedade de declarar ocorrências posteriores.

5.2 está ciente e aceita os regulamentos do Sistema, relativos ao Pregão Eletrônico.

5.3 não se enquadra como Microempresa ou empresa de pequeno porte, e atesta que não irá usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar Federal nº. 123/06.

5.4 não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal.

5.5 cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

5.6 tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

5.7 temos pleno conhecimento das condições necessárias para prestação dos serviços.

5.8 a empresa optou pela não realização da vistoria técnica nas instalações físicas do **SEBRAE SP**, tendo ciência que não poderá alegar em qualquer fase da licitação ou vigência da relação contratual que não realizará os serviços em conformidade com a qualidade e requisitos exigidos e que tem pleno

conhecimento das condições e peculiaridades inerentes à natureza do trabalho, assume total responsabilidade por este fato e não utilizará deste para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a contratante.

5.9 está garantida a exequibilidade da proposta comercial apresentada, assegurando que os preços e condições ofertados refletem a viabilidade técnica e econômica para a execução completa dos serviços/produtos especificados no edital. A proposta considera todos os requisitos exigidos, garantindo a qualidade, os prazos, os recursos e o atendimento às normas legais e regulatórias aplicáveis, visando ao pleno cumprimento do objeto contratado e à satisfação dos critérios de eficiência e economicidade estabelecidos.

5.10 está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega em definitivo.

5.11 cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório.

5.12 não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição.

5.13 nos preços apresentados, já estão computados todos os custos necessários decorrentes do fornecimento de produtos e da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

5.14 para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui Anexo do Edital.

5.15 inexiste qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com servidores ou dirigente do **SEBRAE SP**.

5.16 nos valores propostos estão inclusas todas as despesas, inclusive frete, tributos e encargos de qualquer natureza incidentes sobre o objeto do Edital, nada mais sendo lícito pleitear a esse título.

5.17 por ocasião da assinatura do contrato, disporá de equipe técnica especializada e necessária para execução do futuro contrato.

5.18 estamos de pleno acordo com as condições estabelecidas no Edital e seus anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas nos documentos de contratação.

5.19 a proposta foi elaborada de forma independente.

5.20 sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico Nº **90051/2025**, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

5.21 estamos cientes da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do

cumprimento integral ao que estabelece o art. 6º e seus incisos, da Instrução Normativa nº 01, de 19 de janeiro de 2010.

5.22 a signatária não se encontra suspensa de licitar ou contratar com o SEBRAE SP.

5.23 a produtividade adotada é a utilizada pela Administração como referência.

5.24 além do escopo de fornecimento proposto, não há outros materiais e equipamentos que serão utilizados na execução dos serviços.

5.25 executaremos o contrato e os serviços de acordo com as especificações e condições estabelecidas no Edital e seus Anexos.

5.26 em caso de ausência ou divergência entre qualquer declaração aqui expressa com as requisitadas no Edital e seus Anexos, atesta que está ciente e de acordo com as expressas no Edital e seus anexos.

6 Escopo de Fornecimento

6.1 Fabricantes e Fornecedores

Fornecedor	País	Nome do Representante	E-mail	Telefone	Site
Layer Tecnologia	Brasil	Victor Araújo Freire Rodrigo Garcia Medeiros	comercial@layer.net.br	(61) 3544-7273	https://www.layer.net.br
Cymulate	Israel	Daniel Almeida Gomes	danielg@cymulate.com	(11) 95551-8886	https://cymulate.com/
Cymulate	Israel	Rafael Gonçalves	rafaelg@cymulate.com	(61) 99171-7649	https://cymulate.com/

6.2 Composição

ITEM	DESCRIÇÃO			UND.	QTD ITEM
01	**Solução de gerenciamento de exposição contínua a ameaças. Período de subscrição = 24 meses**			Unidade	01
	Fornecedor: Cymulate	Produto/Serviço: Cymulate Cloud Platform	Versão: n/a		
Subitem	**Código**	**Descrição**			**Qtd. Total**
1	CCP	Cymulate Cloud Platform			1
2	Serviço	Serviço de Instalação			1

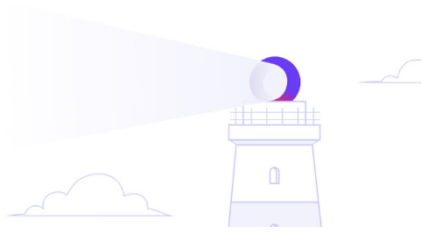
ITEM	DESCRIÇÃO			UND.	QTD ITEM
02	**Licenciamento da capacidade de validação de brechas e simulações de ataques. Período de subscrição: 24 meses**			Usuário	2.600
	Fornecedor: Cymulate	Produto/Serviço: BAS + HOPPER	Versão: n/a		
Subitem	**Descrição**				**Qtd. Total**
1	BAS-2	Breach and Attack Simulation			2.600
2	HOP-2	Hopper			2.600

ITEM	DESCRIÇÃO			UND.	QTD ITEM
03	**Licenciamento da Capacidade de Gestão de Superfície de Ataque Externo. Período de subscrição: 24 meses**			Ativo	2.500
	Fornecedor: Cymulate	Produto/Serviço: ASM	Versão: n/a		
Subitem	**Descrição**				**Qtd. Total**
1	ASM	Attack Surface Management			2.500

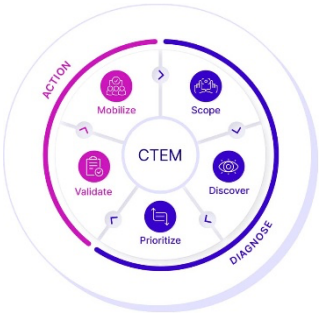
ITEM	DESCRIÇÃO			UND.	QTD ITEM
04	**Serviço de suporte técnico especializado da solução.**			Mês	24
	Fornecedor: Layer	Produto/Serviço: Suporte Técnico	Versão: n/a		
Subitem	**Descrição**				**Qtd. Total**
1	Serviço	Serviço de suporte técnico especializado 24 meses			24

7 Descrição

7.1 ITEM 01 - SOLUÇÃO DE GERENCIAMENTO DE EXPOSIÇÃO CONTÍNUA A AMEAÇAS.



Cymulate Cloud Plataform -CCP é uma plataforma de validação de exposições cibernéticas última geração que permite às organizações **avaliarem continuamente sua postura de segurança cibernética**. Seu design modular oferece uma abordagem abrangente para testes de vulnerabilidades, detecção de ameaças e resposta rápida, aumentando a resiliência contra as ameaças atuais. Entre seus principais componentes estão o **BAS (Breach and Attack Simulation),** que simula cenários de ativos comprometidos para identificar vulnerabilidades exploráveis; o **ASM (Attack Surface Management**), que mapeia e monitora continuamente toda a superfície de ataque da organização, identificando ativos expostos ou desprotegidos e facilitando ações corretivas; e o **Hopper**, um recurso que simula ataques de movimento lateral dentro da rede corporativa, testando a facilidade com que um invasor pode se mover de um computador para outro, contornar defesas e extrair dados.



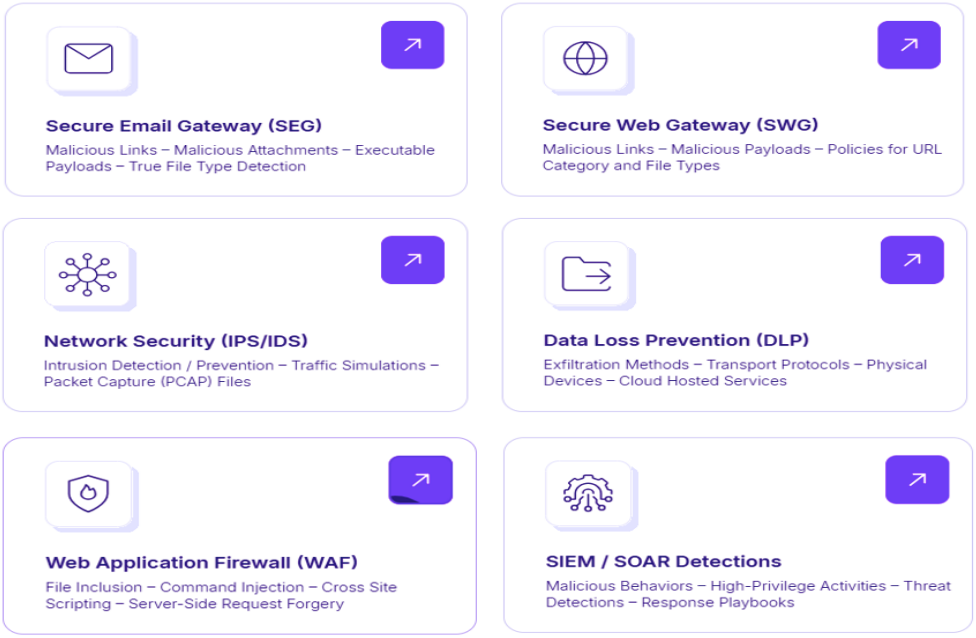
A plataforma Cymulate Cloud Plataform traz a melhor validação de segurança para o centro da análise de exposição em uma plataforma unificada e aberta, que inclui integrações e análises para dar suporte a cada estágio do processo de **gerenciamento contínuo de exposição a ameaças (CTEM).**

A **Cymulate** é reconhecida como fornecedora representante para validação de exposição cibernética. que oferece suporte aos recursos principais, recomendados e opcionais que o **Gartner®** defende no relatório. Além disso, a **Cymulate** foi nomeada pela *Frost & Sullivan* como empresa líder em seu relatório *Frost Radar: Automated Security Validation, 2024*. O relatório avalia o número crescente de organizações e líderes de segurança que recorrem à Validação de Segurança Automatizada (ASV) para avaliar a eficácia de seus controles de segurança e fornecer tendências quantitativas e insights sobre a postura de segurança da organização.

7.2 ITEM 02 - LICENCIAMENTO DA CAPACIDADE DE VALIDAÇÃO DE BRECHAS E SIMULAÇÕES DE ATAQUES.

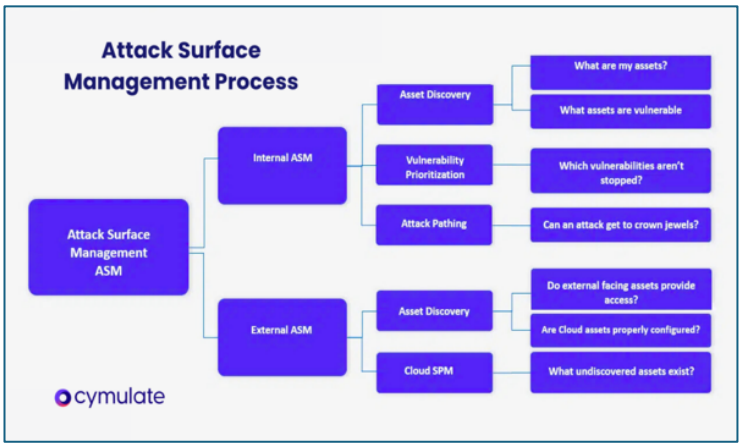
A plataforma **Cymulate Cloud Platform - CCP**, implementa a capacidade de ***Breach and Attack Simulation*** **(BAS)** para **realizar simulações de ataque** contínuas e automatizadas, **mapeando caminhos de ataque** e visualizando o impacto de uma possível violação. Isso permite que as empresas priorizem exposições com base em dados concretos, considerando não apenas a vulnerabilidade em si, mas também o contexto dos ativos afetados, como unidades de negócios, linhas de produtos e regiões geográficas.

A capacidade de validação de brechas e simulações de ataques (BAS) da Cymulate Cloud Plataform automatiza testes para os seguintes controles:



7.3 ITEM 03 - LICENCIAMENTO DA CAPACIDADE DE GESTÃO DE SUPERFÍCIE DE ATAQUE EXTERNO.

A plataforma Cymulate Cloud Platform - CCP, implementa a capacidade de ***External Attack Surface Management (EASM)*** *para* oferecer uma abordagem completa e automatizada para a **gestão da superfície de ataque**. Com recursos que identificam ativos expostos, vulnerabilidades e configurações incorretas, ela permite uma **avaliação contínua e proativa da postura de segurança**, tanto interna quanto externamente.



7.4 ITEM 04 - SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO DA SOLUÇÃO.

Os serviços de suporte técnico especializado serão **sempre realizados em plena conformidade com os requisitos do Edital e seus Anexos**, independente da descrição aqui realizada. O processo de implantação e suporte técnico é efetuado com segurança pelo nosso time de consultores especializados, de forma faseada conforme o fluxo a seguir.

CÓDIGO: B2-6B-8A-AF-BB-C3-A8-A5-BB-9B-75-2E-E5-74-A6-66-6E-02-B2-05-E2

- **Kickoff**:
  - Contempla a apresentação de equipes, escopo de projeto e fases da implantação e definição de pontos focais.

- **Planejamento**:
  - De acordo com a necessidade do projeto, é desenhada a melhor abordagem para o processo de instalação, configuração e disponibilização da solução em produção. Além das estratégias, são definidas questões de arquitetura, plano operacional da instalação e requisitos.

- **Instalação**:
  - Provisionamento do Tenant.

- **Configuração**:
  - Cadastro de usuários administradores;
  - Distribuição dos agentes;
  - Integrações;
  - Outros.

- **Teste**:
  - Após a configuração completa do ambiente, é iniciado um processo de teste completo para certificar que todas as configurações e integrações estão operantes.

- **Migração**:
  - Uma vez testado e verificado, inicia-se a migração da solução.

- **Certificação**:
  - Certificação da solução instalada para sua efetiva operação.

- **Suporte Técnico**:
  - Prestação dos serviços de suporte técnico nos termos do Edital e seus anexos.

8 Comprovações Técnicas

8.1 Nesta seção estão comprovados os requisitos mínimos e obrigatórios para os itens do escopo de fornecimento.

8.2 Consta anexo à presente proposta, documentação técnica (manuais, catálogos oficiais do fabricante, links URL etc.) que comprova o pleno atendimento a todos os requisitos técnicos listados no "**ANEXO ESPECIFICAÇÕES TÉCNICAS MÍNIMAS R OBRIGÁTORIAS**" do Termo de Referência, através de planilha ponto a ponto, com indicação de nome do documento e página que comprovam o atendimento.

8.3 Estamos cientes que a CONTRATANTE poderá a qualquer momento realizar diligência junto a licitante e/ou fabricante para comprovação da veracidade de qualquer documento apresentado.

8.4 Os seguintes documentos são partes integrantes da presente proposta:

- 000-Comprovacao-Ponto-a-Ponto-v2.pdf
- 005-Comprovacao-Tabela-Links.pdf
- 010-Carta-Cymulate-Parceria-Layer.pdf
- 100-CYMULATE-Platforms-Data-Sheet.pdf
- 101-CYMULATE-Implementing-CTEM.pdf
- 102-CYMULATE-Azure-AD-SAML-based-SSO-Integration.pdf
- 103-CYMULATE-Using-OAuth-20-for-API-Authentication.pdf
- 104-CYMULATE-About-cymulate-Integrations.pdf
- 105-CYMULATE-Integration-with-CrowdStrike-Falcon.pdf
- 106-CYMULATE-Cymulate-Installation-Guide.pdf
- 107-CYMULATE-SIEM-Validation-Solution-Brief.pdf
- 108-CYMULATE-Managing-your-agents-in-the-platform.pdf
- 109-CYMULATE-Management-Capabilities.pdf
- 110-CYMULATE-Dashboard.pdf
- 111-CYMULATE-About-Assessment-reports.pdf
- 112-CYMULATE-About-Immediate-Threats-Executive-reports.pdf
- 113-CYMULATE-About-Phishing-Awareness-Campaign-reports.pdf
- 114-CYMULATE-About Environments.pdf
- 115-CYMULATE-About Environments.pdf
- 116-CYMULATE-Managing users.pdf
- 117-CYMULATE-BAS-Advanced-Scenarios_Data-Sheet.pdf
- 118-CYMULATE-BAS-Email-Gateway-Assessment.pdf
- 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf
- 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf
- 121-CYMULATE-About-Hopper-assessments.pdf
- 122-CYMULATE-Lateral-Movement-Assessment.pdf
- 123-CYMULATE-ASM-Data-Sheet.pdf
- 124-CYMULATE-Run-multiple-assessments-in-parallel.pdf
- 125-CYMULATE-About-External-ASM.pdf
- 126-CYMULATE-Scanning-subsidiary-domains-with-Attack-Surface-Management (2).pdf
- 127-CYMULATE-multiple assessments.pdf
- 400-CyberView-DataSheet.pdf

8.5 As seguintes “URLs” são partes integrantes da presente proposta:

Fabricante	URLs
Cymulate	https://4347852.fs1.hubspotusercontent-na1.net/hubfs/4347852/eBook/Implementing%20Continuous%20Threat%20Exposure%20Management%20(CTEM)%20-%20August%2022.pdf
Cymulate	https://cituploads.blob.core.windows.net/channelmechanics/Cymulate/Content%20Program/Product%20URLs/Product%20and%20Technical%20Solutions/Cymulate%20Management%20Capabilities.pdf
Cymulate	https://cituploads.blob.core.windows.net/channelmechanics/Cymulate/Content%20Program/Product%20URLs/Product%20and%20Technical%20Solutions/Email%20Gateway%20Assessment.pdf
Cymulate	https://cituploads.blob.core.windows.net/channelmechanics/Cymulate/Content%20Program/Product%20URLs/Product%20and%20Technical%20Solutions/Lateral%20Movement%20Assessment.pdf
Cymulate	https://cituploads.blob.core.windows.net/channelmechanics/Cymulate/Content%20Program/Product%20URLs/Product%20and%20Technical%20Solutions/Phishing%20Awareness%20Assessment.pdf
Cymulate	https://cituploads.blob.core.windows.net/channelmechanics/Cymulate/Content%20Program/Product%20URLs/Product%20and%20Technical%20Solutions/Web%20Gateway%20Assessment.pdf
Cymulate	https://cymulate.com/blog/cymulates-sigma-rules/
Cymulate	https://cymulate.com/blog/extended-security-posture-management-empowers/
Cymulate	https://cymulate.com/end-user-license-agreement/
Cymulate	https://cymulate.com/mitre-attack/
Cymulate	https://cymulate.com/resources/cymulate-and-rapid7-unite-for-cybersecurity-visibility/

Fabricante	URLs
Cymulate	https://cymulate.com/security-at-cymulate/
Cymulate	https://cymulate.com/solutions/attack-based-vulnerability-prioritization/
Cymulate	https://cymulate.com/solutions/siem-validation/
Cymulate	https://cymulate.com/technology-alliances/
Cymulate	https://cymulate.com/uploaded-files/2019/12/RSA-Archer-Solution-Brief.pdf
Cymulate	https://cymulate.com/uploaded-files/2022/11/BAS-Data-Sheet.pdf
Cymulate	https://cymulate.com/uploaded-files/2023/06/Cymulate-Exposure-Analytics-Data-Sheet.pdf
Cymulate	https://cymulate.com/uploaded-files/2023/08/CART-Data-Sheet.pdf
Cymulate	https://cymulate.com/uploaded-files/2023/08/CART-Data-Sheet.pdf
Cymulate	https://cymulate.com/uploaded-files/2024/03/RBI-Case-Study.pdf
Cymulate	https://cymulate.com/uploaded-files/2024/03/Cymulate-Technology-Partners-and-Ecosystem-Document.pdf
Cymulate	https://cymulate.com/uploaded-files/2024/04/BAS-Advanced-Scenarios_Data-Sheet.pdf
Cymulate	https://cymulate.com/web-application-firewall/
Cymulate	https://l.cymulate.com/hubfs/Cymulate%20-%20Web%20Application%20Firewall%20Solution%20Brief.pdf
Cymulate	https://l.cymulate.com/hubfs/Datasheet/Platforms%20Data%20Sheet.pdf
Cymulate	https://l.cymulate.com/hubfs/Main%20-%202021%20Cymulate%20brochure.pdf
Cymulate	https://l.cymulate.com/hubfs/Solution_Brief/Cymulate%20-%20Data%20Exfiltration%20Assessment%20Solution%20Brief.pdf

8.6 Planilha de Comprovação ponto-a-ponto:

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
1.2.	**ITEM 01: SOLUÇÃO DE GERENCIAMENTO DE EXPOSIÇÃO CONTÍNUA A AMEAÇAS.**			
1.2.1.	Requisitos Gerais:	a) Conforme itens abaixo		
1.2.1.1.	Implantar plataforma base que atenda todos os requisitos técnicos desse item, através de solução de um único fabricante, ou, alternativamente, através de soluções modulares de diversos fabricantes integrados entre si.	a) Ciente e de acordo. b) Proposta Técnica Comercial, Item 1 - Escopo de Fornecimento. c) Proposta Técnica Comercial, Item 2 - Escopo de Fornecimento. d) Proposta Técnica Comercial, Item 3 - Escopo de Fornecimento.	N/A	b) Cymulate Cloud Platform c) Breach and Attack Simulation (BAS) d) External ASM
1.2.1.2.	Possuir licenciamento oficial do fabricante para os softwares e soluções ofertadas. Não será aceito licenciamentos nas seguintes modalidades: "community (free)", "NFR (not for resale)", "demo (demonstração)", open source, e que não disponham de suporte e garantia oficial de atualização junto ao fabricante.	a) Ciente e de acordo. b) Proposta Técnica Comercial, Item 1 - Escopo de Fornecimento. c) Proposta Técnica Comercial, Item 2 - Escopo de Fornecimento. d) Proposta Técnica Comercial, Item 3 - Escopo de Fornecimento. e) https://cymulate.com/end-user-license-agreement/	N/A	b) Cymulate Cloud Platform c) Breach and Attack Simulation (BAS) d) External ASM e) This Agreement forms a legally binding c**ontract between Customer and Cymulate in relation to Customer's use of the Platform**. The Platform also includes all enhancements, modifications, additions, translations, compilations, or other software delivered to Customer by Cymulate hereunder and any and all printed and electronic documentation provided with the Platform.
1.2.1.3.	Fornecer atualizações de versões durante toda a vigência do contrato.	a) https://cymulate.com/end-user-license-agreement/		a) Cymulate may make modifications, additions, and upgrades to the Platform, as it deems necessary. **The terms of this Agreement will apply to any updates that Cymulate may make available** to the Customer unless the update is accompanied by a separate license, in which case that license terms will govern
1.2.1.4.	Possuir representante oficial do(s) fabricante(s) no Brasil.	a) Ciente e de acordo b) 010-Carta-Cymulate-Parceria-Layer.pdf	b) 1	b) Daniel Almeida Gomes - LATAM Sales Director - danielg@cymulate.com
1.2.1.5.	A proposta deve apresentar nome, endereço, telefone e e-mail do representante(s) oficial (ais) no Brasil.	a) Ciente e de acordo. b) Proposta Técnica Comercial	b) 6	b) Daniel Almeida Gomes - danielg@cymulate.com - (11) 95551-8886 b) Rafael Gonçalvesr - rafaelg@cymulate.com - (61) 99171-7649
1.2.1.6.	Implantar funcionalidades que abranja os conceitos de:	a) Conforme itens abaixo		
a)	Validação de brechas e simulações de ataques (BAS),	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - Cymulate Breach and Attack Simulation Cymulate **Breach and Attack Simulation (BAS**) validates cybersecurity controls by safely conducting threat activities, tactics, techniques, and procedures in production environments.
b)	Gestão da superfície de ataque externo (EASM), e,	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 4	a) pg 4 - Cymulate Attack Surface Management **Cymulate Attack Surface Management (ASM)** automates the ongoing process of identifying internal and external assets, showing where security gaps exist, where they can be

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
				used to perform an attack, and where defenses are strong enough to repel an attack.
c)	Mecanismo de detecção de propagação de ameaças na rede.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 5	a) pg 5 - **The network penetration testing** capability simulates an attacker that has gained an initial foothold in a company's network and moves laterally in search of any additional assets that can be compromised.
1.2.1.7.	Fornecer plataforma baseada em modelo nuvem SaaS (Software as a Service). Não serão aceitas soluções do tipo ON-premisse.	a) 101-CYMULATE-Implementing-CTEM.pdf	a) 7	a) pg 7 -The Cymulate Platform is the only **SaaS (Software as a Service)** that unites all the technologies needed to achieve all CTEM validation objectives under a single pane of glass.
1.2.1.8.	Implantar simulação, avaliação e gestão ampliada da postura de segurança da organização, medindo a eficácia por meio de testes e avaliações do nível de proteção tanto do perímetro quanto de ambientes internos, proporcionando uma visão abrangente sobre a efetividade dos controles de segurança.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 1	a) pg 1 -Gain an attackers view of attack surfaces, vulnerabilities, and **security efficacy** to support continuous threat exposure management programs a) pg 2 - Contextualized vulnerability prioritization correlates vulnerability findings (of multi-vendor aggregated data) with **business context and security control effectiveness**.
1.2.1.9.	Implantar capacidade ilimitada de escaneamento/simulações de ataque para as funcionalidades requisitadas neste item, bem como para os quantidades solicitadas nos ITENS 2 e 3 da Tabela 01 – Escopo de Fornecimento.	a) Ciente e de acordo. b) 127-CYMULATE-multiple assessments.pdf	b) 1	b) Yes, you can run multiple assessments at the same time as long as each assessment is executed on a different Test point. ach test point operatesindependently, allowing parallel execution without conflicts. However, if two assessments are configured to use the same test point, one will be queued un□l the other complete
1.2.1.10.	Possuir a capacidade, através de sua rede de inteligência, de fornecer informações sobre ameaças emergentes e relevantes para a plataforma, com detalhes sobre essas ameaças e as medidas de remediação recomendadas.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3- The immediate threat intelligence capability tests security controls against **new and emergent threats observed in the wild**. The Cymulate Threat Research Group updates Cymulate BAS daily with attack simulations of these latest threats that require urgent attention and action. Threat and simulation updates include insights into threat actors, attack vectors, techniques mapped to MITRE ATT&CK, and indicators of compromise.
1.2.1.11.	Permitir que profissionais de cibersegurança identifiquem, diagnostiquem, gerenciem, controlem e validem a postura de segurança cibernética de ponta a ponta.	a) 101-CYMULATE-Implementing-CTEM.pdf	a) 4	a) pg 4 - **Diagnose** – This stage is when the identification and mapping of priorities and weaknesses take place: Scoping – Mapping the external attack surface, listing all digital assets, evaluating their operational values, and conveying that value to all stakeholders so that both technical and executives people understand which assets are defined as high impact. Discovery – ncovering environments' security gaps (such as vulnerabilities and misconfigurations) and their risk profile, and, ideally, mapping them to assets for easy prioritization. Prioritization – **Identifying and addressing** the security gaps most likely to be exploited by cyber-attackers based on an adversarial perspective and correlating the findings to high-impact assets from an organizational or business point of view. B. Action – This stage is when the security posture is tested, and corrective measures are taken: **Validation – The validation step** is tasked with a triple objective: g n a Assess attack success likelihood. Evaluate the attack damage potential beyond gaining an initial foothold. **Verify the effectiveness** of the detection and response existing rray.
1.2.1.12.	Permitir a recriação de cenários reais de ataques à infraestrutura de segurança do SEBRAE-SP.	a) 101-CYMULATE-Implementing-CTEM.pdf	a) 12	a) pg 12 -Each organization has its specificities that no off-the-shelf automation can entirely cover. Purple teams expand BAS int**o creating and automating custom advanced attack scenarios**.
1.2.1.13.	O volume de usuários (ITEM 2) e de Ativos (ITEM 3) para ativar as funcionalidades da plataforma base serão definidos pela contratação e demanda dos quantitativos dos ITENS 2 e 3.	a) Ciente e de acordo		
1.2.1.14.	Fornecer os serviços de instalação, ativação, testes da plataforma base, de forma garantir que a plataforma esteja apta a sua operação e ativação dos licenciamento dos ITENS 2 e 3 da Tabela 01 – Escopo de fornecimento.	a) Ciente e de acordo		
1.2.1.15.	A partir da assinatura do contrato, correrão os seguintes prazos:	a) Conforme itens abaixo		

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
1.2.1.15.1.	Reunião de início do projeto (kick-off): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pelo SEBRAE com 02 (dois) dias úteis de antecedência.	a) Ciente e de acordo		
1.2.1.15.2.	Entrega do Projeto Executivo: até 20 (vinte) dias corridos, contados a partir da reunião de início do projeto (kick-off);	a) Ciente e de acordo		
1.2.1.15.3.	O SEBRAE se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;	a) Ciente e de acordo		
1.2.1.15.4.	Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo SEBRAE, a respeito da manifestação sobre o Projeto Executivo;	a) Ciente e de acordo		
1.2.1.15.5.	A conclusão da fase de implantação dos serviços é de até 60 (sessenta) dias corridos, contados a partir da data de aceite do projeto executivo, mediante a emissão do termo de recebimento definitivo pelo SEBRAE.	a) Ciente e de acordo		
1.2.2.	**Funcionalidades Gerais:**	a) Conforme itens abaixo		
1.2.2.1.	Permitir integração com serviços de SSO, possibilitando autenticação centralizada e login seguro dos usuários na plataforma, com suporte a protocolos SAML 2.0 e OAuth 2.0, para garantir compatibilidade com os principais provedores de identidade.	a) 102-CYMULATE-Azure-AD-SAML-based-SSO-Integration.pdf b) 103-CYMULATE-Using-OAuth-20-for-API-Authentication.pdf	a) 1 b) 1	a) pg 1 - Cymulate supports single sign-on (SSO) logins through **SAML 2.0.** b) pg 1 - Using **OAuth 2.0** for API Authentication
1.2.2.2.	Possuir compatibilidade com APIs de diversas plataformas de segurança, gerenciada por uma console central, ou alternativamente, integradas em diversos módulos, permitindo configurações, monitoramento e atualizações automáticas.	a) 104-CYMULATE-About-cymulate-Integrations.pdf b) 105-CYMULATE-Integration-with-CrowdStrike-Falcon.pdf	a) 1 b) 1	a) pg 1 - **Cymulate integrates with various technology partner**s to augment and benefit exis ng security solu ons. You can integrate your Endpoint detec on and response (**EDR**), Security Informa on and Event Management (**SIEM**), Vulnerability Management (**VM**), and other solutions with Cymulate to automate security controls valida on, priori ze remedia on plans, manage security tasks, and more. B) pg 1 - The Cymulate agent queries the Crowdstrike **API** to fetch detec on and alert data
1.2.2.3.	Permitir o auto provisionamento de usuários para garantia de autenticação e autorização através de grupos do AD (Active Directory). Este processo poderá ser feito via API ou interface gráfica, deste que, seja nativo do fabricante.	a) 102-CYMULATE-Azure-AD-SAML-based-SSO-Integration.pdf	a) 1 a 21	a) pg 1 - Cymulate supports single sign-on (SSO) logins through SAML 2.0. A SAML 2.0 iden ty provider (IDP) can take many forms, one of which is a self-hosted **Active Directory** Federation Services (AD FS) server. AD FS is a service provided by Microso as a standard role for Windows Server that provides a web login using existing Active Directory credentials. a) pg 18 - **Configuring SSO in the Cymulate Platform Configuring SSO in the Cymulate Platform**
1.2.2.4.	Permitir comunicação entre componentes via proxy web, com protocolos seguros como HTTPS e TLS 1.2 ou superiores.	a) https://cymulate.com/security-at-cymulate/	a) Encryp tion	a) All communications with Cymulate UI and APIs are encrypted via industry standard **HTTPS/TLS (TLS 1.2 or higher)** over public networks. This ensures that all traffic between Cymulate and its customers is secure during transit. Transport Layer Security (TLS) encrypts and delivers email securely, mitigating eavesdropping between mail servers where peer services support this protocol.
1.2.2.5.	Permitir a instalação de agentes de forma manual, automatizada ou em lote.	106-CYMULATE-Cymulate-Installation-Guide.pdf	a) 5	a) pg 5 -You can use the command line interface to expedite the installation process by suppressing some or all of the dialog boxes that appear during a GUI installation. This becomes particularly useful w**hen installing multiple instances of Cymulate agen**t.
1.2.2.6.	Fornecer níveis de risco após cada simulação, comparando resultados atuais e anteriores para determinar progresso ou retrocesso, e estabelecer um baseline.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 2	a) pg 2 - Mobilize new security programs **with benchmarks and baselines** a) pg 3 - Each vector is scored independently and aggregated for an **overall risk score based on industry-standard frameworks**.
1.2.2.7.	Permitir a criação de regras “SIGMA” e permitir a conversão dessas regras em buscas (queries) para plataformas de “SIEM” ou criação de regras de correlação.	a) 101-CYMULATE-Implementing-CTEM.pdf b) 107-CYMULATE-SIEM-Validation-Solution-Brief.pdf	a) 8 b) 2	a) pg 8 - Actionable mitigation guidance, **including pre-encoded sigma rules**, is available for uncovered security gaps. b) pg 2 - Optmize **SIEM with Automated Sigma Rules** and Remediation Guidance
1.2.2.8.	Permitir integrações com tecnologias de segurança, proporcionando maior visibilidade em detecção, gestão de vulnerabilidades, automação de “playbooks” e validação de processos internos.	a) 101-CYMULATE-Implementing-CTEM.pdf b) 104-CYMULATE-About-cymulate-Integrations.pdf	a) 12 b) 1	a) pg 12 - Custom scenarios can be used to exercise **incident response playbooks**, pro-active threat hunting, and automate security assurance procedures and health checks. B) pg 1 - Cymulate integrates with various technology partners to augment and benefit exis ng security solu ons. You can integrate your Endpoint detec on and response (EDR), Security Informa on and

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
				Event Management (SIEM), Vulnerability Management (VM), and other solutions with Cymulate to automate security controls valida on, priori ze remedia on plans, manage security tasks, and more.
1.2.2.9.	Possuir compatibilidade com soluções de correlação de eventos "SIEM" para os produtos de segurança que não possuem integração direta.	a) 107-CYMULATE-SIEM-Validation-Solution-Brief.pdf	a) 1	a) pg 1 - C**ymulate easily integrates with the leading SIEM platforms** to run assessments that validate whether the SIEM is accurately detecting relevant threats and properly alerting security analysts
1.2.2.10.	Permitir à conversão de regras "SIGMA" para o "SIEM" da Securonix atualmente em uso na SEBRAE.	a) 107-CYMULATE-SIEM-Validation-Solution-Brief.pdf b) https://cymulate.com/blog/cymulates-sigma-rules/	a) 2	a) Quadro de Imagens com a logo da **Securonix** b) Why Cymulate's Off-the-Shel**f Sigma Rules** are a Game-Changer for SOC Teams
1.2.2.11.	Fornecer visibilidade do status e versão dos agentes, permitindo ações como reinicialização ou desinstalação via console.	a) 108-CYMULATE-Managing-your-agents-in-the-platform.pdf	a) 1	a) pg 1 - **Restart an agent , Uninstall an agent**
1.2.2.12.	Permitir avaliar a eficácia das defesas da organização contra táticas e procedimentos de grupos criminosos conhecidos, com uma biblioteca atualizada automaticamente com ameaças emergentes.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - The full kill-chain scenarios capability simulates end-to-end attack scenarios of known **advanced persistent threat (APT) groups and potential campaigns.** a) pg 3 - Cymulate Breach and Attack Simulation (BAS) validates cybersecurity controls by safely conducting threat activities, **tactics, techniques, and procedure**s in production environments.
1.2.2.13.	Permitir a criação de perfis de adversários e oferecer simulações de ataques baseados nos frameworks MITRE ATTACK e TTPs disponíveis.	a) 101-CYMULATE-Implementing-CTEM.pdf	a) 5	a) pg 5 - Even though Cymulate's automations cover the **entire MITRE TTPs list,** its advanced purple teaming framework enables the easy creation of additional attack templates that can be created with an easy drag-and-drop type interface.
1.2.2.14.	Possuir console de gerenciamento com dashboard que apresente informações sobre vulnerabilidades baseadas em ataques, incluindo:	a) 109-CYMULATE-Management-Capabilities.pdf b) 128-CYMULATE-Navigating-the-platform.pdf c) Conforme itens abaixo	a) 2 b) 7	a) pg 2 - The **pre-loaded Attack-Based Vulnerability Management (ABVM) dashboard** empowers security managers to rapidly reach educated decisions in their security strategy, prioritize workloads, substantially reduce risk, and minimize costs. b) pg 71 - Analyze and prioritize vulnerabilities with contextual insights, enabling targeted and effective remedia on efforts.
1.2.2.14.1.	a opção de rastreabilidade dos testes em tempo de execução.	a) 110-CYMULATE-Dashboard.pdf	a) 3	a) pg 3 - The Traces widget displays all updates and actions for the most recently run assessment per module. When an assessment is running, the Traces widget displays **the traces in real me**
1.2.2.14.2.	interface para o gerenciamento dos ataques em andamento, visualização de logs e configurações de recursos envolvidos no ataque, incluindo proxy, e-mail, entre outros.	a) 110-CYMULATE-Dashboard.pdf b) 101-CYMULATE-Implementing-CTEM.pdf	a) 1 b) 7	a) pg 1 - The Cymulate dashboard presents an **at-a-glance view of all modules**, their scores, as well as the overall Cymulate security posture score. You can view dashboards per environment by selecting an environment from the dropdown list. a) pg 7 - The Cymulate Platform is the only SaaS (Software as a Service) that unites all the technologies needed to achieve all CTEM validation objectives **under a single pane of glass**.
1.2.2.15.	Permitir a geração de relatórios técnicos ou gerenciais.	a) 111-CYMULATE-About-Assessment*reports.pdf b) 112-CYMULATE-About-Immediate-Threats-Executive-reports.pdf	a) 1 b) 1	a) pg 1 - On the Assessment Reports page, you can access d**etailed reports for each module** b) pg 1 - Cymulate Immediate Threats executive reports are designed to provide high-level, actionable information that can be **used by executives and other decisionmakers** within an organization to assess and improve their cybersecurity strategy.
1.2.2.16.	Permitir a extração de dados completos em sua guia de relatórios, com informações gerais de todos os ataques realizados em um determinado vetor, além da opção de download dos relatórios em formatos PDF, CSV ou TXT.	a) 112-CYMULATE-About-Immediate-Threats-Executive-reports.pdf b) 113-CYMULATE-About-Phishing-Awareness-Campaign-reports.pdf	a) 1 b) 2	a) pg 1 - Click Generate Report Generate Report and **select Executive (PDF)** b) pg 2 - GENERATE REPORT – Click to generate Execu ve reports (**email, PDF, CSV).**
1.2.2.17.	Permitir a geração e download de relatórios via interface e permitir o envio por e-mail.	b) 113-CYMULATE-About-Phishing-Awareness-Campaign-reports.pdf	a) 1	a) pg 2 - GENERATE REPORT – Click to generate Execu ve reports (**email**, PDF, CSV).
1.2.2.18.	Implantar a geração de relatórios e uma visão detalhada segmentada por ambientes.	a) 114-CYMULATE-About Environments.pdf	a) 2	a) pg 2 - You can **view reports for each environment.**
1.2.2.19.	Implantar uma visão clara do desempenho individual de cada vetor de ataque, incluindo um gráfico de comparação para benchmark.	a) 111-CYMULATE-About-Assessment*reports.pdf	a) 2 e 3	a) pg 2 - **Benchmark** – View benchmark data for the selected module. a) pg 3 - IMAGEM.
1.2.2.20.	Fornecer um caminho simplificado para, no mínimo:	a) Conforme itens abaixo		
1.2.2.20.1.	Abrir chamados.	a) 115-CYMULATE-About Environments.pdf	a) 11	a) pg 11 - **Contact Support**
1.2.2.20.2.	Gerenciar usuários da plataforma.	a) 116-CYMULATE-Managing users.pdf	a) 1	a) pg 1 - The **User Management page** allows you to manage all users in the

CÓDIGO: B2-6B-8A-A9-BB-C3-A8-A8-BB-9B-75-2E-E5-74-A8-66-6E-02-B2-05-B2

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
				Cymulate pla orm. You can add new users, edit user details, export users, and set roles, preferences, and permissions.
1.2.2.20.3.	Acessar documentações do produto.	a) 115-CYMULATE-About Environments.pdf	a) 11	a) pg 11 - **Knowledge Base**
1.2.2.20.4.	Gerenciar logs e atividades em execução.	a) 115-CYMULATE-About Environments.pdf	a) 9 e 10	a) pg 12 - **Activity log** - Lists all activities performed by users on the platform a) pg 10 - The No fications tab displays notifications for Immediate Threats, Cymulate scores, and other important alerts for the user.
1.2.3.	**Funcionalidades de Validação de Brechas e Simulações de Ataques (BAS):**	a) Conforme itens abaixo		
1.2.3.1.	Implantar simulações automáticas, voltadas para a avaliação de ajustes e configurações de diferentes controles de segurança.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - Cymulate Breach and Attack Simulation (BAS) **validates cybersecurity controls** by safely conducting threat activities, tactics, techniques, and procedures in production environments.
1.2.3.2.	Implantar validação de controles de segurança, para no mínimo, as seguintes ferramentas de proteção:	a) 100-CYMULATE-Platforms-Data-Sheet.pdf b) Conforme itens abaixo	a) 3	a) pg 3 - Cymulate Breach and Attack Simulation (BAS) **validates cybersecurity controls** by safely conducting threat activities, tactics, techniques, and procedures in production environments.
1.2.3.2.1.	Soluções de Proteção de Endpoints (Endpoint Protection/EDR) .	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - **Endpoint Security**
1.2.3.2.2.	Gateway de E-mail Seguro (Mail Gateway Security).	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - **Email Gateway**
1.2.3.2.3.	Gateway de Web Seguro (Secure Web Gateway).	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - **Web Gateway**
1.2.3.2.4.	Firewall de Aplicação Web Seguro (Web Application Firewall).	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - **Web Application Firewall**
1.2.3.2.5.	DLP (Data Loss Prevention).	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 -**Data Exfiltration**
1.2.3.3.	Implantar simulações de ataque através de um agente único ao qual deverá ser capaz de executar ataques em diferentes vetores de forma individual ou simultânea.	a) 117-CYMULATE-BAS-Advanced-Scenarios_Data-Sheet.pdf	a) 1	a) pg 1 - Cymulate BAS Advanced Scenarios is a SaaS-based solution that **uses a single lightweight agent** per environment to run automated assessments of on-prem, cloud, or hybrid environments.
1.2.3.4.	Permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma isolada, além de possibilitar simulações que respeitem o ciclo de vida completo de um ataque.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - Cymulate BAS Advanced Scenarios enables red teams to **create and automate custom attack simulations**. Applying the MITRE ATT&CK® framework, security teams use BAS Advanced Scenarios to create complex scenarios from both pre-built resources and custom binaries and executions
1.2.3.5.	Permitir identificar quais testes foram bem-sucedidos e quais falharam durante o processo de prevenção. Para os resultados, deve ser possível gerar evidências de detecção e/ou bloqueio através de integração com um SIEM e/ou diretamente no dispositivo que detectou e/ou bloqueou a simulação.	a) 107-CYMULATE-SIEM-Validation-Solution-Brief	a) 2	a) pg 2 - The Cymulate Exposure Management Platform includes breach and attack simulation to automate production-safe security assessments that determine **if your SIEM is accurately detecting various attack scenario**s and high privilege behaviors
1.2.3.6.	Implantar as simulações a partir de componentes da solução ou de um equipamento dedicado exclusivamente a simulação.	a) 101-CYMULATE-Implementing-CTEM.pdf	a) 11	a) pg 11- There are **two main methodological approaches** to continuous security validation: **with agents and without agent**s. In other words, from the inside or outside in. Each method has its pros and cons, and a holistic continuous security validation program should ideally include both.
1.2.3.7.	Permitir que ao concluir ataques, seja com vetores de ataque individualmente ou em conjunto, apresentar um score de risco com uma visão clara da maturidade atual e histórica do ambiente.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3- **Each vector is scored independently** and aggregated for an overall risk score based on industry-standard frameworks.
1.2.3.8.	Permitir para a validação do vetor de endpoint, simulações de ataque para:	a) Conforme itens abaixo		
1.2.3.8.1.	Ransomware: Avaliação da eficácia dos recursos para detecção de comportamentos anômalos durante a execução segura de ransomwares, que devem buscar arquivos sensíveis no host e usar chaves geradas de forma controlada para criptografia de arquivos.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - The full kill-chain scenarios capability simulates end-to-end attack scenarios of known advanced persistent threat (APT) groups and potential campaigns. These attack simulations deliver and execute production-safe **ransomware**, trojan, worm, or ustom payloads via web or email attack;
1.2.3.8.2.	Worm: Avaliação da eficácia dos recursos para detecção de comportamentos anômalos durante a execução segura de worms, que devem realizar a descoberta de hosts vulneráveis e simular a proliferação por meio de protocolos, como SMB.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - The full kill-chain scenarios capability simulates end-to-end attack scenarios of known advanced persistent threat (APT) groups and potential campaigns. These attack simulations deliver and execute production-safe ransomware, trojan, **worm**, or ustom payloads via web or email attack;
1.2.3.8.3.	Trojan: Avaliação da eficácia dos recursos para detecção de comportamentos anômalos durante a execução segura de trojans, com coleta de informações do host, como nome de usuário e e-mail, além da possibilidade de estabelecer comunicação usando métodos diversos de reverse shell.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - The full kill-chain scenarios capability simulates end-to-end attack scenarios of known advanced persistent threat (APT) groups and potential campaigns. These attack simulations deliver and execute production-safe

CÓDIGO: B2-6B-8A-A9-BB-C3-A8-A8-BB-9B-95-2E-E5-74-A8-66-6E-02-B2-05-B2

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
				ransomware, **trojan**, worm, or ustom payloads via web or email attack;
1.2.3.8.4.	Antivírus: Avaliação da eficácia de inspeção e proteção contra ameaças de arquivos maliciosos, com malwares em disco sendo atualizados diariamente por meio de múltiplos feeds de segurança.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - **Endpoint Security**
1.2.3.8.5.	MITRE ATT&CK: Avaliação da eficácia dos recursos anti-malware com comandos customizados que simulam o comportamento de adversários conforme o framework ATT&CK.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf	a) 3	a) pg 3 - Cymulate Threat Research Group with daily updates on emergent threats and new simulations – all mapped to the **MITRE ATT&CK** Framework.
1.2.3.9.	Permitir para validação do vetor de e-mail gateway, simulações de ataque para:	a) 100-CYMULATE-Platforms-Data-Sheet.pdf b) Conforme itens abaixo	a) 3	a) pg 3 - **Email Gateway**
1.2.3.9.1.	Ransomware: Avaliação dos recursos de proteção de e-mail com técnicas de execução de ransomwares, em execução segura. Worm: Avaliação dos recursos de proteção de e-mail com técnicas de execução de worms, de forma segura.	a) 118-CYMULATE-BAS-Email-Gateway-Assessment.pdf	a) 1	a) pg 1 - **Ransomware**
1.2.3.9.2.	Malware: Avaliação de proteção de e-mail com execução de malwares, simulando cenários interativos, como UAC, roubo de credenciais e C&C.	a) 118-CYMULATE-BAS-Email-Gateway-Assessment.pdf b) 129-CYMULATE-Email-Gateway-Validation-Solution-Brief.pdf	a) 1	a) pg 1 - **Malicious link** b) pg 1- s**imulates different types of e-mail based threats with the latest ransonware, malware, worms, trojans and exploits delivered**
1.2.3.9.3.	Payload: Avaliação dos recursos de proteção de e-mail com técnicas de execução de payloads em ambiente seguro.	a) 118-CYMULATE-BAS-Email-Gateway-Assessment.pdf	a) 1	
1.2.3.9.4.	Exploits: Avaliação dos recursos de proteção de e-mail com execução de arquivos que exploram vulnerabilidades em programas.	a) 118-CYMULATE-BAS-Email-Gateway-Assessment.pdf	a) 1	a) pg 1 - **Exploit**
1.2.3.9.5.	Dummy: Avaliação dos recursos de proteção de e-mail utilizando payloads conhecidos, como MessageBox do Metasploit, em ambiente seguro.	a) 118-CYMULATE-BAS-Email-Gateway-Assessment.pdf b) 129-CYMULATE-Email-Gateway-Validation-Solution-Brief.pdf	a) 2 b) 1	a) pg 2 - The agent collects the results and **deletes malicious payloads** from the mailbox. Test Results and Remediation b) pg 1- simulates different types of e-mai**l based threats with the latest ransonware, malware, worms, trojans and exploits delivered**
1.2.3.9.6.	True File Type Detection: Avaliação da proteção de e-mail com envio de arquivos cuja extensão difere do formato original, para identificar possíveis brechas.	a) https://cymulate.com/blog/security-validation-best-practices-email-gateways/		a) **True File Type Detection** - This final test is used to validate that your email gateway can detect the actual type of file that has been attached to an email regardless of the file extension. Threat actors often disguise malicious files with misleading file extensions to avoid detection by the email gateway. Instead of relying solely on the file extension, true file type detection examines the actual contents of the file to identify its real format. As such, we need to validate the ability of your email gateway to detect the true file type and block malicious files from being sent to users.
1.2.3.10.	Permitir para validação do vetor de web application firewall (WAF), simulações de ataque para:	a) 100-CYMULATE-Platforms-Data-Sheet.pdf b) Conforme itens abaixo	a) 3	a) pg 3 - **Web Application Firewall**
1.2.3.10.1.	SQL Injection.	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf	a) 1	a) pg 1 - **SQL injection**
1.2.3.10.2.	Cross-site Scripting (XSS).	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf	a) 1	a) pg 1 - **Cross-site scripting (XSS)**
1.2.3.10.3.	NoSQL Injection.	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf b) https://cymulate.com/solution-brief/cymulate-waf-solution-brief/	a) 1	a) pg 1 - and **other forms of command injections** are used toexploit web application and web infrastructurevulnerabilities that can lead to a breach b) SQL/**NoSQL injection**
1.2.3.10.4.	XML Injection.	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf b) https://cymulate.com/solution-brief/cymulate-waf-solution-brief/	a) 1	a) pg 1 - and **other forms of command injections** are used toexploit web application and web infrastructurevulnerabilities that can lead to a breach b) **XML Injection**
1.2.3.10.5.	Path Traversal.	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf b) https://cymulate.com/solution-brief/cymulate-waf-solution-brief/	a) 1	a) pg 1 - Leverage Cymulate's extensive library of web attack types to test your WAF security efficacy against thousands of payloads mapped to **OWASP TOP 10.** **b) Path (directory) traversal**
1.2.3.10.6.	Inclusão de Arquivo para Execução Remota de Código.	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf b) https://cymulate.com/solution-brief/cymulate-waf-solution-brief/	a) 1	a) pg 1 - File inclusion for **remote code execution** b) **File inclusion**
1.2.3.10.7.	Injeção de Comando.	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf b) https://cymulate.com/solution-brief/cymulate-waf-solution-brief/	a) 1	a) pg 1 - **Command injection** b) **Command injection**
1.2.3.10.8.	WAF Bypass.	a) 119-CYMULATE-Web-Application-Firewall-Solution-Brief.pdf b) https://cymulate.com/solution-brief/cymulate-waf-solution-brief/	a) 1	a) pg 1 - Leverage Cymulate's extensive library of web attack types to test your WAF security efficacy against thousands of payloads mapped to **OWASP TOP 10.** b) **WAF bypass**
1.2.3.11.	Permitir para validação de vazamento de dados (DLP), simulações de ataque para os métodos abaixo:	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - Challenging Your **DLP Controls Cymulate's** Data Exfiltration vector enables you to test the effectiveness of your **Data Loss Prevention (DLP)** security controls and optimize them.

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
1.2.3.11.1.	HTTP & HTTPS: Exfiltração de dados por HTTP/S, injetando dados confidenciais nos cabeçalhos de solicitação enviados a um servidor remoto.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **HTTP & HTTPS**
1.2.3.11.2.	Navegadores HTTP & HTTPS: Exfiltração de dados via navegadores como IE, Edge e/ou Chrome.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **HTTP & HTTPS**
1.2.3.11.3.	DNS: Exfiltração de dados pela porta 53.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **DNS & DNS Tunneling**
1.2.3.11.4.	Tunelamento DNS: Exfiltração via protocolo DNS, com injeção de dados em solicitações DNS.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **DNS & DNS Tunneling**
1.2.3.11.5.	Tunelamento ICMP: Exfiltração usando cabeçalhos ICMP com pacotes ECHO para um servidor remoto.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **ICMP Tunneling.**
1.2.3.11.6.	Telnet: Exfiltração pela porta 23 do Telnet.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - Once initiated, the Cymulate Agent will attempt to exfiltrate information using **all the combinations of data types and exfiltration methods** defined in the test-template.
1.2.3.11.7.	SFTP: Exfiltração pelo protocolo SFTP.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **Secure File Transfer Protocol**
1.2.3.11.8.	Outras Portas: Exfiltração via upload de dados para servidores externos por portas abertas.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - Once initiated, the Cymulate Agent will attempt to exfiltrate information using **all the combinations of data types and exfiltration methods** defined in the test-template.
1.2.3.11.9.	Email: Exfiltração usando e-mail corporativo no Outlook.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **Email**
1.2.3.11.10.	Serviços de Nuvem: Exfiltração para ou através de aplicativos e serviços em nuvem.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **Cloud Services**
1.2.3.11.11.	Dispositivos Removíveis: Exfiltração via cópia para dispositivos removíveis, como USB.	a) 120-CYMULATE-Data-Exfiltration-Solution-Brief.pdf b) Conforme itens abaixo	a) 1	a) pg 1 - **Removable Device (USB)**
1.2.4.	**Funcionalidades de Detecção de Propagação de Ameaças na Rede:**	a) 121-CYMULATE-About-Hopper-assessments.pdf b) Conforme itens abaixo.	a) 1	a) pg 1 - Once an a acker gains an ini al foothold in a network, their next objective is to **move laterally** and gain access to more systems and sensitive data.
1.2.4.1.	Implantar recursos para avaliar o impacto de políticas de segmentação de rede e a eficácia de controles internos contra a movimentação lateral.	a) 121-CYMULATE-About-Hopper-assessments.pdf	a) 1	a) pg 1 - Once an a acker gains an ini al foothold in a network, their next objective is to **move laterally** and gain access to more systems and sensitive data.
1.2.4.2.	Possuir a capacidade de simular movimentos de ataque em tempo real, visando identificar e explorar pontos de fragilidade que permitam o movimento não autorizado entre segmentos da rede.	a) 121-CYMULATE-About-Hopper-assessments.pdf	a) 1	a) pg 1 - Cymulate Hopper assessments **test your internal network configuration and segmentation** policies against the various techniques and methods that a ackers use to spread within a network and gain control over additional systems.
1.2.4.3.	Permitir simulações de ataque para a verificação dos seguintes métodos:	a) Conforme itens abaixo.		
1.2.4.3.1.	Pass-the-Password.	a) https://cymulate.com/cybersecurity-glossary/credential-dumping/		a) Attackers frequently use techniques like **pass-the-hash** or pass-the-ticket**.** These allow them to inject stolen hashes or Kerberos tickets into sessions and navigate across systems as if they were authorized users. a) Validating the efficacy of those pre-emptive measures can be done by using automated lateral movement technologies such as Cymulate Continuous Automated Red Teaming (CART) with its Hopper module that simulates an attacker that has gained an initial foothold and moves laterally in search of any additional assets that can be compromised.
1.2.4.3.2.	Pass-the-Ticket.	a) https://cymulate.com/cybersecurity-glossary/credential-dumping/		a) Attackers frequently use techniques like pass-the-hash or **pass-the-ticket.** These allow them to inject stolen hashes or Kerberos tickets into sessions and navigate across systems as if they were authorized users. a) Validating the efficacy of those pre-emptive measures can be done by using automated lateral movement technologies such as Cymulate Continuous Automated Red Teaming (CART) with its Hopper module that simulates an attacker that has gained an initial foothold and moves laterally in search of any additional assets that can be compromised.
1.2.4.3.3.	Pass-the-Hash.	a) https://cymulate.com/blog/mitigate_lateral_movement_iam_network_segmentation/		a) Pass the Hash a) Validating the efficacy of those pre-emptive measures can be done by using automated lateral movement technologies such as Cymulate Continuous Automated Red Teaming (CART) with its Hopper module that simulates an attacker that has gained an initial foothold and moves laterally in

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
				search of any additional assets that can be compromised.
1.2.4.3.4.	Brute Force.	a) https://cymulate.com/cybersecurity-glossary/credential-compromise/		a) **Brute-force attacks:** a) The Cymulate Security Validation and Exposure Management Platform simulates thousands upon thousands of cyber-attacks to verify that zero trust segmentation functions as intended. It continuously assesses segmentation from multiple perspectives and provides actionable insights to strengthen security postures.
1.2.4.3.5.	LLMNR/NBT-NS Poisoning and Relay.	a) https://cymulate.com/blog/mitigate_lateral_movement_iam_network_segmentation/		a) **LLMNR Poisoning** a) Validating the efficacy of those pre-emptive measures **can be done by using automated lateral movement technologies such as Cymulate Continuous Automated Red Teaming (CART) with its Hopper module** that simulates an attacker that has gained an initial foothold and moves laterally in search of any additional assets that can be compromised.
1.2.4.3.6.	Kerberoast.	a) https://cymulate.com/blog/mitigate_lateral_movement_iam_network_segmentation/		a) **Kerberoasting** a) Validating the efficacy of those pre-emptive measures **can be done by using automated lateral movement technologies such as Cymulate Continuous Automated Red Teaming (CART) with its Hopper module** that simulates an attacker that has gained an initial foothold and moves laterally in search of any additional assets that can be compromised.
1.2.4.3.7.	Password Spraying.	a) https://cymulate.com/blog/mitigate_lateral_movement_iam_network_segmentation/		a) Brute-force attacks: Hackers use automated tools to guess weak passwords (also known as **password spraying**). a) Validating the efficacy of those pre-emptive measures can be done by using automated lateral movement technologies such as Cymulate Continuous Automated Red Teaming (CART) with its Hopper module that simulates an attacker that has gained an initial foothold and moves laterally in search of any additional assets that can be compromised.
1.2.4.3.8.	Roubo de senhas LAPS.	a) https://cymulate.com/cybersecurity-glossary/credential-dumping/		a) Secrets sprawl also invites attack: store admin passwords securely **(e.g. with Microsoft's LAPS)** and avoid shared accounts. a) Cymulate's Hopper module ensures a safe testing environment by utilizing non-destructive attack methods exclusively. These methods include activities like credential dumping, pass the hash, and kerberoasting.
1.2.4.4.	Permitir a criação de modelos personalizados nos vetores de ataque, sem impactar o ambiente.	a) 100-CYMULATE-Platforms-Data-Sheet.pdf b) 101-CYMULATE-Implementing-CTEM.pdf	a) 3 b) 12	a) pg 3 - Cymulate BAS tests the effectiveness of **various security controls across the entire cyber kill-chain** – from attack delivery to exploitation and post-exploitation b) pg 12 - Each organization has its specificities that no off-the-shelf automation can entirely cover. Purple teams expand BAS into **creating and automating custom advanced attack scenarios**.
1.2.4.5.	Possuir recursos para configurar e adaptar o comportamento de testes para simular diferentes vetores de ataque, permitindo uma avaliação detalhada da resposta do ambiente a movimentações laterais	a) 100-CYMULATE-Platforms-Data-Sheet.pdf b) 101-CYMULATE-Implementing-CTEM.pdf	a) 3 b) 12	a) pg 3 - Cymulate BAS tests the effectiveness of **various security controls across the entire cyber kill-chain** – from attack delivery to exploitation and post-exploitation b) pg 12 - Each organization has its specificities that no off-the-shelf automation can entirely cover. Purple teams expand BAS into **creating and automating custom advanced attack scenarios**.
1.2.4.6.	Permitir que o agente da solução atue de forma idêntica a um atacante real, sem necessidade de outros agentes para validar diferentes métodos.	a) 117-CYMULATE-BAS-Advanced-Scenarios_Data-Sheet.pdf b) 130-CYMULATE-About-Hopper-assessments.pdf	a) 1 b) 1	a) pg 1 - Cymulate BAS Advanced Scenarios is a SaaS-based solution that **uses a single lightweight agent** per environment to run automated assessments of on-prem, cloud, or hybrid environments. b) pg 1- The Hopper assessment simulates the actions of an attacker who has taken control of a single compromised workstation and attempts to spread throughout the organization
1.2.4.7.	Permitir o "pivoting" na rede, fornecendo um mapa completo da trilha percorrida e dos	a) 122-CYMULATE-Lateral-Movement-Assessment.pdf	a) 1	a) pg 1 - Based on results from previous stages, the Cymulate Agent will try to

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
	alvos alcançados, permitindo a identificação de alvos que podem ser considerados joias da coroa (Crown Jewels) ou não.			spread laterally from the original workstation by leveraging one or more attack methods. **If Crown Jewels have been defined** in the template, the campaign will attempt to access these specifically.
1.2.5.	**Funcionalidades de Gerenciamento de Superfície de Ataque Externo:**	a) 123-CYMULATE-ASM-Data-Sheet.pdf b) Conforme itens abaixo.	a) 1	a) pg 1 - Attack Surface Management (ASM)
1.2.5.1.	Permitir identificar automaticamente ativos externos da organização, como domínios, subdomínios, IPs, servidores expostos e outras interfaces públicas, que possam ser alvos de ataques.	a) 123-CYMULATE-ASM-Data-Sheet.pdf	a) 1	a) pg 1 - Cymulate's ASM technology discovers which digital assets are exposed to adversaries to access, exploit, and collect information uring the reconnaissance phase of an attack. I**t scans the domains, subdomains, IPs, ports, etc., for internet-facing vulnerabilities** and or Open-Source Intelligence (OSINT).
1.2.5.2.	Implantar varreduras contínuas para detectar novos ativos e mudanças no ambiente externo da organização, proporcionando visibilidade em tempo real das possíveis vulnerabilidades e riscos.	a) 123-CYMULATE-ASM-Data-Sheet.pdf	a) 2	a) pg 2 - **Continuous, automated checkups Swift evaluations** lead to prompt adjustments based on up-to date informatio
1.2.5.3.	Permitir classificar e priorizar as vulnerabilidades descobertas com base no risco que representam para a organização, levando em conta o impacto e a criticidade dos ativos.	a) 123-CYMULATE-ASM-Data-Sheet.pdf	a) 2	a) pg 2 - **Prioritize discovered vulnerabilities** and misconfigurations.
1.2.5.4.	Permitir monitorar a internet e a dark web em busca de possíveis vazamentos de dados sensíveis da organização, como credenciais comprometidas ou outras informações críticas.	a) 123-CYMULATE-ASM-Data-Sheet.pdf	a) 2	a) pg 2- **Clear-Web & Dark Web** Compromised User Information/ Credentials.
1.2.5.5.	Permitir a consolidação das informações de ativos, vulnerabilidades e riscos em um painel unificado, facilitando a gestão e resposta aos problemas identificados.	a) 123-CYMULATE-ASM-Data-Sheet.pdf	a) 2	a) pg 2 - Overall Score Security score based on simulated attack success rate correlated with industry standards Top Findings **At a glance, expandable, view of top attacks, top assets and top finding**
1.2.5.6.	Permitir a automação de alertas e a geração de relatórios personalizados, notificando os responsáveis pelas áreas de segurança sobre novos riscos ou vulnerabilidades descobertas.	a) 125-CYMULATE-About-External-ASM.pdf	a) 1	a) pg 1 - The results of the full scan include a **detailed report of discovered assets, vulnerability findings, and a risk score** to help organizations prioritize their mitigation efforts effectively. a) pg 1 - All findings generated in the scans are presented in a dashboard with a complete view of all exposed and accessible assets external to the organiza on's perimeter, along with a risk assessment score. T**he security team can then take appropriate measures to reduce their risk exposure.**
1.2.5.7.	Permitir simular ataques externos contra a organização para avaliar a eficácia dos controles de segurança e identificar pontos fracos na defesa.	a) 126-CYMULATE-Scanning-subsidiary-domains-with-Attack-Surface-Management.pdf	a) 1	a) pg 1 -The Cymulate Attack Surface Management (ASM) Relationships module is designed to **enhance the identification and management of an organization's attack surface**. This module employs a systematic approach to analyze a root domain and then identify related subsidiary domains and their respective assets.
1.2.5.8.	Entregável:	a) Conforme itens abaixo		
1.2.5.8.1.	Apresentar evidências da ativação da plataforma no formato SaaS.	a) Ciente e de acordo		
1.2.5.8.2.	Relatório as-built da ativação da plataforma em nome do SEBRAE.	a) Ciente e de acordo		
1.3.	**ITEM 02: LICENCIAMENTO DA CAPACIDADE DE VALIDAÇÃO DE BRECHAS E SIMULAÇÕES DE ATAQUES.**			
1.3.1.	Métrica: Cada "usuário" ou "agente" representa 1 (um) unidade de licenciamento desse item.	a) Ciente e de acordo		
1.3.1.1.	Permitir que o licenciamento seja dimensionado conforme o número de usuários ou agentes nos quais a simulação de segurança será aplicada, visando cobrir áreas críticas da infraestrutura organizacional.	a) https://cymulate.com/end-user-license-agreement/ b) https://cymulate.com/terms-of-use/	a) 1	a) In the event that the actual **number of assets used by the Customer** is higher than the number indicated in the License Certificate, the Customer shall pay Cymulate an additional subscription fee pro-rated to the Fee indicated in the Quote or such other order form executed between Cymulate and the Customer. Such additional fee shall be part of the Fee. b) In addition, **the number of assets or employees of the Customer**, as applicable, shall be reevaluated by Cymulate at the end of the Initial Term and any renewal term thereafter, and the subscription fee may be increased by Cymulate to reflect such new number of assets or employees, based on Cymulate's then current price list. Notwithstanding anything to the

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
				contrary, any renewal in which the packages, number of assets, number of employees, number of vectors or subscription term, as applicable, had decreased from the prior subscription term will result in re-pricing at renewal without regard to the subscription fee paid for the prior subscription term.
1.3.2.	Permitir a realização de simulações ilimitadas e automatizadas de ataques cibernéticos no ambiente do SEBRAE para o número de usuários definidos no escopo de fornecimento.	a) 127-CYMULATE-multiple assessments.pdf	a) 1	a) **Yes, you can run multiple assessments at the same time** as long as each assessment is executed on a different Test point. ach test point operatesindependently, **allowing parallel execution without conflicts**. However, if two assessments are configured to use the same test point, one will be queued un□l the other complete
1.3.2.1.	O licenciamento desse item ativa as funcionalidades de software das seções "Funcionalidades de Validação de Brechas e Simulações de Ataques (BAS)" e "Funcionalidades de Detecção de Propagação de Ameaças na Rede" do ITEM 01 da Tabela 1 – Escopo de fornecimento.	a) Ciente e de acordo		
1.3.3.	Entregável:	a) Conforme itens abaixo		
1.3.3.1.	Relatório as-built com evidências da ativação na plataforma do ITEM 01 do volume de licenças adquiridas através do ITEM 02.	a) Ciente e de acordo		
1.4.	**ITEM 03: LICENCIAMENTO DA CAPACIDADE DE GESTÃO DE SUPERFÍCIE DE ATAQUE EXTERNO.**			
1.4.1.	Métrica: Cada "ativo" ou "asset" representa 1 (um) unidade de licenciamento desse item.	a) Ciente e de acordo		
1.4.1.1.	Permitir que o licenciamento seja baseado na quantidade de ativos monitorados, sendo que cada ativo se refere a um componente digital externo (ex.: subdomínios, endereços IP públicos IPV4 e IPV6, ASN, e-mails, web services, aplicativos web) que compõe a superfície de ataque exposta.	a) a) 123-CYMULATE-ASM-Data-Sheet.pdf b) https://cymulate.com/end-user-license-agreement/ c) https://cymulate.com/terms-of-use/	a) 1	a) pg 1 - Cymulate's ASM technology discovers which digital assets are exposed to adversaries to access, exploit, and collect information uring the reconnaissance phase of an attack. I**t scans the domains, subdomains, IPs, ports, etc., for internet-facing vulnerabilities** and or Open-Source Intelligence (OSINT). b) In the event that the actual **number of assets used by the Customer** is higher than the number indicated in the License Certificate, the Customer shall pay Cymulate an additional subscription fee pro-rated to the Fee indicated in the Quote or such other order form executed between Cymulate and the Customer. Such additional fee shall be part of the Fee. c) In addition, **the number of assets or employees of the Customer**, as applicable, shall be reevaluated by Cymulate at the end of the Initial Term and any renewal term thereafter, and the subscription fee may be increased by Cymulate to reflect such new number of assets or employees, based on Cymulate's then current price list. Notwithstanding anything to the contrary, any renewal in which the packages, number of assets, number of employees, number of vectors or subscription term, as applicable, had decreased from the prior subscription term will result in re-pricing at renewal without regard to the subscription fee paid for the prior subscription term.
1.4.1.2.	Permitir o monitoramento dos ativos digitais expostos encontrados pelo módulo de Gestão de Superfície de Ataque Externo, garantindo a segurança e a continuidade operacional da organização.	a) 123-CYMULATE-ASM-Data-Sheet.pdf	a) 1	a) pg 1 - **Automated scanning and discovery of public-facing and internal systems.** The Cymulate ASM module scans organizations' xternal and internal surfaces to identify exposed assets. a) pg 1 - Definition of **exposed assets and platforms Discovered assets** and platforms are described to facilitate a rapid understanding of the data collected.
1.4.1.3.	O licenciamento desse item ativa as funcionalidades de software da seção "Funcionalidades de Gerenciamento de Superfície de Ataque Externo" do ITEM 01 da Tabela 1 – Escopo de fornecimento.	a) Ciente e de acordo		
1.4.1.4.	Entregável:	a) Conforme itens abaixo		
1.4.1.4.1.	Relatório as-built com evidências da ativação na plataforma do ITEM 01 do volume de licenças adquiridas através do ITEM 03.	a) Ciente e de acordo		
1.5.	**ITEM 04: SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO DA SOLUÇÃO.**			

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
1.5.1.	O serviço de suporte técnico especializado para a solução deve prever assistência técnica contínua e personalizada, garantindo que o SEBRAE maximize o valor da solução contratada.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.2.	O serviço deve possuir alinhamento ao programa de Gerenciamento Contínuo de Ameaças (CTEM) do Gartner, contemplando as seguintes etapas: definição do escopo, descoberta, priorização, validação e mobilização. Figura 1 - Etapas do Serviço de Suporte Especializado	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.3.	As atividades de suporte técnico especializado do programa de CTEM a serem realizadas pela CONTRATADA devem contemplar os seguintes objetivos e atividades:	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.	Definição do Escopo	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.1.	Objetivo	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.1.1.	Definir claramente os objetivos do programa de CTEM e o resultado desejado, alinhando-os com a visão estratégica do SEBRAE. Esta fase é crucial para que o processo de CTEM a ameaças seja direcionado e focado, permitindo uma proteção eficaz dos ativos mais críticos.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.2.	Atividades	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.2.1.	Implantar uma definição do escopo de atuação da solução de CTEM.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.2.2.	Implantar a coleta de informações de contato dos usuários, equipes técnicas e de segurança para garantir uma integração eficiente.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.2.3.	Implantar o estabelecimento de KPIs para acompanhar a evolução da solução.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.	Descoberta	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.1.	Objetivo	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.1.1.	Coletar dados e informações para entender o estado atual de exposição à riscos cibernéticos e seus impactos no SEBRAE. Esta fase busca criar um inventário abrangente dos ativos, serviços, sistemas e suas potenciais falhas de segurança, formando a base para as fases subsequentes de priorização e mobilização.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.2.	Atividades	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.2.1.	Implantar o mapeamento de ativos visando identificar os ativos críticos, incluindo sistemas, redes, dispositivos e aplicações.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.2.2.	Implantar a avaliação das áreas de exposição que podem ser exploradas por atacantes, como interfaces externas e serviços acessíveis pela internet.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.2.3.	Implantar o mapeamento de possíveis caminhos de ataque.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.3.2.4.	Implantar a identificação de vulnerabilidades e exposições descobertas para que possam ser priorizadas e tratadas nas próximas fases.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.	Priorização	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.1.	Objetivo	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.1.1.	Priorizar as ameaças e falhas de segurança mais críticas de acordo com a criticidade e o impacto potencial que representam para o SEBRAE. Esta fase é essencial para que a equipe de segurança possa concentrar esforços nas ameaças que oferecem maior risco, otimizando o uso de recursos para reduzir a superfície de ataque de forma eficiente.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.2.	Atividades	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.2.1.	Implantar análise das ameaças para entender como as vulnerabilidades podem impactar o SEBRAE.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.2.2.	Implantar avaliação do impacto potencial de cada ameaça ou vulnerabilidade nos ativos críticos.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.2.3.	Implantar, em conjunto com o SEBRAE, um nível aceitável de risco de segurança e revisá-lo periodicamente para garantir que esteja dentro dos limites estabelecidos.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.4.2.4.	Fornecer um plano preliminar de mitigação com foco nas ameaças e vulnerabilidades mais críticas.	a) Ciente e de acordo		

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
1.5.4.5.	Validação	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.5.1.	Objetivo	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.5.1.1.	Testar e validar a efetividade dos controles de segurança. Esta fase envolve a validação das suposições sobre vulnerabilidades e o cenário de ameaças feitas nas três fases anteriores. Confirma vulnerabilidades, vetores de ataque e a eficácia da estratégia de resposta a incidentes.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.5.2.	Atividades	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.5.2.1.	Implantar testes de simulação de ataque visando a validação dos controles de segurança vigentes.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.5.2.2.	Implantar avaliação da probabilidade de sucesso de um ataque validando se os invasores conseguem realmente explorar os pontos fracos identificados, separando problemas críticos de falsos positivos. Implantar avaliação do plano de resposta a incidentes para validar se os atuais controles de segurança e procedimentos de resposta a incidentes da organização são suficientes para impedir ataques reais direcionados a esses pontos fracos.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.6.	Mobilização	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.6.1.	Objetivo	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.6.1.1.	Mobilizar a equipe técnica do SEBRAE para a garantir que as equipes operacionalizem as remediações por meio de ações claras. Esta fase envolve garantir que os usuários, ferramentas e processos estejam alinhados e prontos para enfrentar as ameaças identificadas de maneira proativa e coordenada.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.6.2.	Atividades	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.6.2.1.	Implantar reuniões periódicas (minimamente mensais) com a equipe técnica do SEBRAE para avaliar o progresso e fornecer recomendações para melhorar a postura de segurança.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.6.2.2.	Implantar revisões estratégicas periódicas (minimamente trimestrais) consolidadas, apresentando relatórios executivos e resultados detalhados das avaliações realizadas.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.6.2.3.	Fornecer apoio na análise de dados e resultados das avaliações, de forma a extrair percepções estratégicas para a tomada de decisões de segurança.	a) Ciente e de acordo		
1.5.4.6.2.4.	Fornecer relatórios executivos periódicas (minimamente trimestrais), detalhando os resultados e oferecendo percepções para a melhoria contínua da segurança cibernética.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.7.	O serviço deverá ainda:	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.7.1.	Fornecer desde a reinstalação e configuração da solução até a resolução de problemas e otimização de processos, permitindo a manutenção de uma postura proativa contra ameaças cibernéticas.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.7.2.	Implantar métodos para configurar permissões de usuário e notificações de acordo com o licenciamento.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.7.3.	Fornecer assistência na instalação de agentes e resolução de possíveis problemas da plataforma.	a) Ciente e de acordo		
1.5.4.7.4.	Fornecer repasse de conhecimento semestral, com carga horária mínima de 8 horas, para até 4 profissionais do SEBRAE, cobrindo configurações e gerenciamento da solução.	a) Ciente e de acordo		
1.5.4.7.5.	Implantar métodos de revisão e refinamento do uso da plataforma, de forma a alinhar as práticas do SEBRAE com as melhores práticas de mitigação de riscos.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.7.6.	Implantar métodos que garantam que as notificações e alertas da plataforma sejam configuradas para apenas os usuários autorizados.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.7.7.	Fornecer documentação detalhada, do tipo As-Built, para apoiar o SEBRAE na avaliação do funcionamento da solução.	a) Ciente e de acordo		
1.5.4.7.8.	Fornecer suporte remoto contínuo, ou on-site quando necessário, para permitir que o SEBRAE resolva dúvidas ou problemas de uso.	a) Ciente e de acordo		

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
1.5.4.7.9.	Implantar métodos para garantir que todos os usuários administradores da plataforma estejam cientes das permissões e responsabilidades dentro do sistema, minimizando erros operacionais.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.7.10.	Implantar serviço de painéis (dashboards) executivos, com indicadores de performance, segurança, operação e administração da solução, de forma que permita o SEBRAE monitorar a execução dos serviços prestados.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.8.	Deverá ainda:	a) Conforme itens abaixo		
1.5.4.8.1.	Implantar o serviço no formato SaaS em nuvem.	a) 400-CyberView-DataSheet	a) 1	a) pg 1 - **Arquitetura SaaS em Nuvem**
1.5.4.8.2.	É de responsabilidade da CONTRATADA a definição, criação e manutenção dos indicadores e painéis, de forma que o SEBRAE possa consumir os painéis prontos.	a) 400-CyberView-DataSheet	a) 1 b) 2 c) 3	a) pg 1 - Painéis Interativos b) pg 2 - Painéis e Dashboards c) pg 3 - A criação dos painéis é realizada em conformidade com a necessidade do cliente e de acordo com os dados que estão disponíveis nos recursos de TI integrados a plataforma.
1.5.4.8.3.	Permitir acesso através de interface Web (HTTPS), com controle de acesso por identificação de usuário e solicitação de senha e duplo fator de autenticação, ambos de forma individual por usuário através de Software Token ("tokens baseados em software").	a) 400-CyberView-DataSheet	a) 1 b) 2	a) pg 1 - Acesso seguro por HTTPS, autenticação por usuário/senha e duplo fator de autenticação com suporte a Soft Token. b) pg 2 - O acesso seguro é realizado por HTTPS, com identificação do usuário por CPF e/ou e-mail e autenticação por senha e duplo fator de autenticação com suporte a App Token, tais como: Google Authenticator, Microsoft Authenticator, Authy, e outros.
1.5.4.8.4.	Possuir recurso de "reset" de senha, de forma que que o usuário receba por e-mail, link para reset da senha ou nova senha temporária de acesso.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - É disponibilizado recurso de reset de senha, onde o usuário recebe um e-mail com senha temporária que permite o acesso a plataforma para cadastro de nova senha e novo QR CODE do Soft Token.
1.5.4.8.5.	Permitir o cadastramento de no mínimo 05 (usuários) do SEBRAE para visualização dos painéis disponibilizados.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Plataforma com arquitetura Multitenancy e capaz de gerenciar múltiplos usuários por tenancy.
1.5.4.8.6.	Possuir tecnologia do tipo responsiva, de forma que a visualização se adapte ao tamanho da tela dos dispositivos utilizados no acesso.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Plataforma com design moderno, elegante e responsivo para Desktops, Tablets e Smartphones.
1.5.4.8.7.	Implantar controle de acesso por usuário, de forma a controlar o grupo de assunto ou painel que pode ser visualizado.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - O controle de acesso aos painéis de indicadores é realizado individualmente por usuário para determinar quais painéis podem ser visualizados.
1.5.4.8.8.	Possuir a capacidade de coleta de dados de forma agendada, recorrente e automática.	a) 400-CyberView-DataSheet	a) 3 b) 3	a) pg 3 - Através de uma estrutura avançada de conectores, a plataforma coleta, higieniza, transforma, enriquece e cataloga grandes volumes de dados de várias fontes, incluindo arquivos em repositório na nuvem, feeds, bancos de dados em nuvem, aplicativos e recursos diversos de TI. b) pg 3 - As coletas poder ser agendadas em frequências diversas, tais como, minuto, hora, dia, semanal, mensal, anual ou customizada.
1.5.4.8.9.	Permitir a visualização gráfica de indicadores por tabelas, KPIs, gráficos, texto formatados, através de:	a) 400-CyberView-DataSheet	a) 2 b) 2	a) pg 2 - Caixa de texto formatada com **suporte a imagem e código HTML**. b) pg 2 - A formatação das caixas de texto, widgets, gráficos e tabelas permitem ajustes de **tipo de fonte, cor do texto e fundo, bordas**, tamanho de fonte, tipo de destaque em negrito / itálico /sublinhado, formatação numérica, moeda, alinhamento, eixos de valores e outros.
1.5.4.8.9.1.	Caixas de Textos, permitindo a inclusão de imagens, HTML e formatações de fonte, borda e cores.	a) 400-CyberView-DataSheet	a) 2 b) 2	a) pg 2 - Caixa de texto formatada com **suporte a imagem e código HTML**. b) pg 2 - A formatação das caixas de texto, widgets, gráficos e tabelas permitem ajustes de **tipo de fonte, cor do texto e fundo, bordas**, tamanho de fonte, tipo de destaque em negrito / itálico /sublinhado, formatação numérica, moeda, alinhamento, eixos de valores e outros.
1.5.4.8.9.2.	KPIs (key performance indicators).	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - **KPIs**/Widgets do tipo Rótulo/Valor com 1º valor, Rótulo/Valor com 1º e 2º valor, Rótulo/Valor com 1º, 2º e 3º valor, Rótulo/Valor comparativo, marcadores horizontais com destino e intervalo mínimo/máximo, e discagem completo.
1.5.4.8.9.3.	Tabelas (Linha x Coluna).	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Tabelas em 2 dimensões do tipo resumo e tabela dinâmica.

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
1.5.4.8.9.4.	Gráficos, com diversos tipos de gráficos (pizza, barras, linha, dispersão, bolha, área).	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Gráficos do tipo funil, localizado, **pizza**, campainha, semicircular, semianel, **linha** com e sem marcadores, etapa, linha suave com e sem marcadores, barra vertical e horizontal, borboleta, histograma, **barra** vertical e horizontal empilhada, **barra** vertical e horizontal 100% empilhadas, barra com linha, barra com **bolha**, barra com dispersão, barra com área, área com **bolha**, linha com **bolha**, combinação personalizada, dispersão, **bolha**, **bolhas** empilhadas, nuvem de palavras, Heat Map, área com e sem marcadores, área suave com e sem marcadores, área empilhada com e sem marcadores, área empilhada suave com e sem marcadores. Suporta a inclusão de legendas e títulos. Suporta previsão de tendências nos gráficos de linha.
1.5.4.8.10.	Permitir filtro interno e individualizado por painel, através de:	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Nossos designers podem criar para cada cliente, filtros de dados poderosos e customizados em tempo de desenvolvimento de cada painel. Dependendo dos tipos dos campos de dados, é possível filtrar por intervalos numéricos específicos, intervalos de datas específicas/sazonais/relativas, valores individuais, topN, bottomN e outros. A plataforma suporta a aplicação de vários filtros (com base em várias colunas) em um painel ou indicador específico.
1.5.4.8.10.1.	um ou mais campos de dados.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Nossos designers podem criar para cada cliente, filtros de dados poderosos e customizados em tempo de desenvolvimento de cada painel. Dependendo dos tipos dos campos de dados, é possível filtrar por intervalos numéricos específicos, intervalos de datas específicas/sazonais/relativas, valores individuais, topN, bottomN e outros. A plataforma suporta a aplicação de vários filtros (com base em várias colunas) em um painel ou indicador específico.
1.5.4.8.10.2.	valores individuais a cada campo incluído no filtro.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Nossos designers podem criar para cada cliente, filtros de dados poderosos e customizados em tempo de desenvolvimento de cada painel. Dependendo dos tipos dos campos de dados, é possível filtrar por intervalos numéricos específicos, intervalos de datas específicas/sazonais/relativas, valores individuais, topN, bottomN e outros. A plataforma suporta a aplicação de vários filtros (com base em várias colunas) em um painel ou indicador específico.
1.5.4.8.10.3.	intervalos do tipo acima de, abaixo de, entre valor inicial e final.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Faixas: Esta opção permite filtrar dados com base em faixas numéricas segmentadas. Ex: 0 a 100, 101 a 200, acima de 10, abaixo de 10 etc.
1.5.4.8.10.4.	Top N e Down N.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - N Superior/Inferior: Esta opção permite classificar os registros e filtrar um número definido N de registros Superior/Inferior. a) pg 2 -N% superior/inferior: N% superior/inferior é semelhante à opção N superior/inferior, exceto que retorna N% dos valores da coluna. Por exemplo, Top 15%, filtrará os 15% principais valores da coluna.
1.5.4.8.10.5.	contagem normal e distinta.	a) 400-CyberView-DataSheet	a) 3	a) pg 3 - Operações matemáticas com filtros: § Filtros podem ser aplicados para auxiliar em operações matemáticas do tipo soma, contagem, contagem distinta, média, mediana, desvio padrão, valor mínimo/máximo, modo, variação etc.
1.5.4.8.10.6.	soma, valor máximo, valor mínimo, média, mediana e valor real.	a) 400-CyberView-DataSheet	a) 3	a) pg 3 - Operações matemáticas com filtros: § Filtros podem ser aplicados para auxiliar em operações matemáticas do tipo soma, contagem, contagem distinta, média, mediana, desvio padrão, valor mínimo/máximo, modo, variação etc.
1.5.4.8.10.7.	data através dos critérios de filtro por ano, trimestre, mês, dia, semana, dia da semana, dia do mês, data real, data e hora real, hora e intervalos entre datas.	a) 400-CyberView-DataSheet	a) 2	a) pg 2 - Valores Reais: Ano - filtra valores de data com base em anos específicos; Trimestre - filtra valores de data com base em trimestres específicos; Mês - filtra valores de data com base em meses específicos; Semana - filtra valores de data com base em semanas específicas;

CÓDIGO: B2-6B-8A-A9-9B-C3-A8-A6-BB-9B-95-2E-E5-74-A8-66-6E-02-5B-05B2

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
				Data - filtra com base em valores de data específica; Data e hora - filtra com base em valores de data e hora específicos; Intervalos - filtra valores com base em intervalos de datas específicas. a) pg 2 - Sazonal: Trimestre - filtra os valores de data com base nos trimestres presentes em todos os anos na coluna. Por exemplo, T1, T2.; Mês - filtra valores de data com base em meses em todos os anos. Por exemplo, janeiro, fevereiro; Semana - filtra valores de data com base em semanas em todos os anos. Por exemplo, Semana 1, Semana 2; Dia da semana - filtra valores de data com base no dia da semana em todos os anos. Por exemplo, domingo, segunda-feira; Dia do mês - filtra valores de data com base no dia do mês em todas as datas.
1.5.4.8.11.	Permitir a seleção de filtros relacionados ao indicador ou ao painel através de campos diversos. A seleção deve ser realizada em caixa de seleção individual ou de múltiplos valores para cada filtro.	a) 400-CyberView-DataSheet	a) 3	a) pg 3 - Para campos do tipo texto é possível selecionar um único valor ou múltiplos valores de filtro. Para campos numéricos/moeda é possível selecionar por valores individuais, faixas, N superior/inferior, N% superior/inferior. Por fim, para campos do tipo data é possível selecionar período entre datas, período atual (ano, mês, dia etc.), período relativo e período sazonal.
1.5.4.8.12.	Permitir a exportação de indicadores gráficos no formato de imagem ou pdf.	a) 400-CyberView-DataSheet	a) 3	a) pg 3 - Exporte gráficos em momento de exibição de forma simples e rápida. Em poucos cliques é possível exportar gráficos em PDF, imagem, excel, csv e HTML. No momento da exportação é possível definir o nome do arquivo e senha de proteção (para alguns formatos a senha será aplicada no arquivo zip exportado).
1.5.4.8.13.	Permitir a definição de senha para posterior acesso ao arquivo exportado.	a) 400-CyberView-DataSheet	a) 3	a) pg 3 - Exporte gráficos em momento de exibição de forma simples e rápida. Em poucos cliques é possível exportar gráficos em PDF, imagem, excel, csv e HTML. No momento da exportação é possível definir o nome do arquivo e senha de proteção (para alguns formatos a senha será aplicada no arquivo zip exportado).
1.5.4.8.14.	A LICITANTE deve informar a plataforma a ser utilizada, bem como apresentar comprovação do atendimento dos requisitos.	a) Ciente e de acordo b) 400-CyberView-DataSheet	b) 1	b) pg 1 - Plataforma de Indicadores CyberView
1.5.4.9.	Implantar todos os requisitos descritos no ITEM 2- DOS REQUISITOS MÍNIMOS E OBRIGATÓRIOS DOS SERVIÇOS DE GARANTIA E SUPORTE.	a) Ciente e de acordo b) Proposta Técnica Comercial, Item 4 - Escopo de Fornecimento.		
1.5.4.10.	Entregável:	a) Conforme itens abaixo		
1.5.4.10.1.1.	Relatórios periódicos, minimamente mensais e trimestrais, com o detalhamento dos serviços executados.	a) Ciente e de acordo		
2.	**DOS REQUISITOS MÍNIMOS E OBRIGATÓRIOS DOS SERVIÇOS DE GARANTIA E SUPORTE**	a) Ciente e de acordo		
	Os serviços de garantia e suporte devem ser prestados pela CONTRATADA, nos seguintes termos.	a) Ciente e de acordo		
	Entende-se por “Garantia” ou “Suporte” ou “Manutenção”, doravante denominada unicamente como “Garantia”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de prestação de serviços. Esta possui suas causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços, tais como:	a) Ciente e de acordo		
	Do hardware: quando aplicável, incluir à desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.	a) Ciente e de acordo		
	Do software: quando aplicável, incluir à desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de	a) Ciente e de acordo		

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
	desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados.			
	Quanto às atualizações pertinentes aos softwares: Entende-se como “atualização” o provimento de toda e qualquer evolução de software, oficial e comprovadamente disponibilizada pelo fabricante da solução, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a necessidade de atualização de tais versões ocorra durante o período contratado.	a) Ciente e de acordo		
	A CONTRATADA aplicará pacotes de correção oficiais do fabricante, em data e horário a serem definidos pelo SEBRAE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato.	a) Ciente e de acordo		
	O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software, independente da severidade do chamado.	a) Ciente e de acordo		
	É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de “Garantia” do tipo “Preventiva” que pela sua natureza reduza a incidência de problemas que possam gerar “Garantia” do tipo “Corretiva”.	a) Ciente e de acordo		
	A manutenção técnica do tipo “corretiva” será realizada sempre que solicitada pelo SEBRAE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA via telefone (com número do tipo “0800” caso a Central de Atendimento esteja fora de São Paulo - SP) ou Internet ou e-mail ou outra forma de contato.	a) Ciente e de acordo		
	Os serviços de “Garantia” incluem:	a) Ciente e de acordo		
	Solução de problemas relativos à indisponibilidade da solução.	a) Ciente e de acordo		
	Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros.	a) Ciente e de acordo		
	Esclarecimento de dúvidas sobre a prestação dos serviços.	a) Ciente e de acordo		
	Instalação de novas versões ou atualizações e patches. Esse serviço deverá ser realizado em horário a ser definido pelo SEBRAE.	a) Ciente e de acordo		
	A CONTRATADA deve disponibilizar a central atendimento 24 horas por dia, 7 dias da semana e equipe com conhecimentos sólidos no serviço prestado.	a) Ciente e de acordo		
	O serviço de “Garantia” deve disponibilizar os seguintes tipos de atendimento:	a) Ciente e de acordo		
	Nível I - Atendimento Telefônico (Help Desk): chamados abertos através de ligação telefônica ou e-mail ou outra forma de contato, em regime de 24x7: 24 horas por dia, 7 dias da semana. Esse serviço deve atender demandas dos usuários referentes ao serviço prestado.	a) Ciente e de acordo		
	Nível II - Atendimento Remoto: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pelo SEBRAE, mediante prévia autorização e seguindo os padrões de segurança do SEBRAE, objetivando análise e solução remota dos problemas apresentados.	a) Ciente e de acordo		
	Nível III - Atendimento Presencial (On-Site): quando aplicável, os atendimentos técnicos realizados nas dependências do SEBRAE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto.	a) Ciente e de acordo		
	Toda “Garantia” deve ser solicitada inicialmente via Help Desk (Nível I), ficando a transferência do atendimento para o Atendimento Remoto (Nível II) condicionado à autorização do SEBRAE.	a) Ciente e de acordo		
	Toda “Garantia” solicitada inicialmente via Help Desk (Nível I), deve ser transferido para o Atendimento Presencial (Nível III) quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.	a) Ciente e de acordo		

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
	Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte Acordo de Níveis de Serviços (ANS) e sua SEVERIDADE:	a) Ciente e de acordo		
	SEVERIDADE URGENTE – Solução totalmente inoperante.	a) Ciente e de acordo		
	Prazo máximo de início de atendimento de até 01 hora úteis contadas a partir do horário de abertura do chamado.	a) Ciente e de acordo		
	Prazo máximo de resolução do problema de até 12 horas úteis contadas a partir do início do atendimento.	a) Ciente e de acordo		
	SEVERIDADE IMPORTANTE – Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.	a) Ciente e de acordo		
	Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado.	a) Ciente e de acordo		
	Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.	a) Ciente e de acordo		
	SEVERIDADE NORMAL – Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.	a) Ciente e de acordo		
	Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado.	a) Ciente e de acordo		
	Prazo máximo de resolução do problema de até 48 horas úteis contadas a partir do início do atendimento.	a) Ciente e de acordo		
	SEVERIDADE EXTERNO – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não disponibilizado pela CONTRATADA.	a) Ciente e de acordo		
	Neste caso, ficam suspensos todos os prazos de atendimento até que o SEBRAE resolva os problemas externos que provocam a inoperância da solução. Após o SEBRAE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.	a) Ciente e de acordo		
	SEVERIDADE INFORMAÇÃO – Solicitações de informações diversas ou dúvidas sobre a solução.	a) Ciente e de acordo		
	Prazo máximo de resposta de até 2 dias úteis, contados a partir da data de abertura da ocorrência.	a) Ciente e de acordo		
	Um chamado técnico somente poderá ser fechado após a confirmação do responsável do SEBRAE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde está instalado.	a) Ciente e de acordo		
	Na abertura de chamados técnicos, será informado pelo SEBRAE a severidade do chamado.	a) Ciente e de acordo		
	A severidade do chamado poderá ser reavaliada pelo SEBRAE, quando verificado que foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.	a) Ciente e de acordo		
	A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.	a) Ciente e de acordo		
	A quantidade de chamados atendidos será agrupada em dois índices, calculados separadamente, conforme abaixo:	a) Ciente e de acordo		
	Indicador de Início de Atendimento (IIA): Mostra o nível de cumprimento do prazo previsto para início de atendimento dos chamados de Atendimento. Deve ser apurado separadamente, por linha de serviço, conforme serviços que estejam em uso pelo SEBRAE:	a) Ciente e de acordo		
	Tabela Indicador IIA	a) Ciente e de acordo		
	Indicador de Tempo de Solução de Atendimento (ITSA): Mostra o nível de cumprimento dos prazos previstos para tempo de solução dos chamados de Atendimento. Deve ser apurado separadamente, por linha de serviço, conforme serviços que estejam em uso pelo SEBRAE:	a) Ciente e de acordo		
	Tablea Indicador ITSAE	a) Ciente e de acordo		

	DESCRIÇÃO DO ITEM	LINK ou DOCUMENTO	Pg.	Trecho
	No mês de apuração, a soma dos valores de desconto dos indicadores IIA e ITSA será descontada do valor devido pela prestação de serviços, limitado a 10%.	a) Ciente e de acordo		
	Os primeiros 90 (noventa) dias a partir da primeira entrega serão considerados como período de estabilização e de ajustes específicos. Durante esse período, o ANS poderão ser flexibilizados por concordância entre as partes.	a) Ciente e de acordo		
	A partir do 91º (nonagésimo primeiro) a partir da primeira entrega, todo o passivo de problemas evidenciado deverá estar solucionado, cabendo a aplicação do nível de serviço sobre o passivo não solucionado e cuja responsabilidade seja exclusivamente da CONTRATADA.	a) Ciente e de acordo		
	A cada 3 meses, os ANS poderão ser revistos em comum acordo entre as partes, baseado nos indicadores de atendimento. Esse acordo será firmado mediante nota técnica emitida pela UTIC e respectiva carta de resposta com a concordância da CONTRATADA.	a) Ciente e de acordo		
	Dentro do prazo máximo de início de atendimento, cabe a CONTRATADA acionar o FABRICANTE para execução das providências que serão adotadas para a solução do chamado.	a) Ciente e de acordo		
	A interrupção dos serviços de atendimento para chamados de severidades 1 e 2 é vedada até o completo restabelecimento de todas as funções do sistema indisponível.	a) Ciente e de acordo		
	Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependam de:	a) Ciente e de acordo		
	Correção de falhas (bugs) pelo Fabricante.	a) Ciente e de acordo		
	Liberação de novas versões e patches de correção da solução pelo Fabricante.	a) Ciente e de acordo		
	Correção de falhas na infraestrutura de TI de responsabilidade do SEBRAE.	a) Ciente e de acordo		
	Correção de falhas de integração da solução com produtos de terceiros não fornecidos pela CONTRATADA.	a) Ciente e de acordo		

Conecte o presente, proteja o futuro.

obrigado!

SHN Qd. 1 - Bloco A - Salas 708/709 – Ed. Le Quartier - Asa Norte
Brasília – DF - 70.701-010
(61) 3544-7273
www.layer.net.br

PROTOCOLO DE ASSINATURA(S)

Proc. 0084-25 - Ameaça Cibernática - Contrato de fornecimento v2

O documento acima foi proposto para assinatura digital através da plataforma de assinaturas do SEBRAE. Para verificar a autenticidade das assinaturas clique neste link https://assinaturadigital.sebrae.com.br/verificadorassinaturas/#/search?codigo=92-9D-8A-6F-9B-C3-A8-DC-03-9F-9F-CF-70-74-A6-69-65-02-B2-5B acesse o site https://assinaturadigital.sebrae.com.br/verificadorassinaturas/#/search e digite o código abaixo:

CÓDIGO: 92-9D-8A-6F-9B-C3-A8-DC-03-9F-9F-CF-70-74-A6-69-65-02-B2-5B

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status é(são):

Carlos Kazunari Takahashi - 374.*.***-37** - 03/10/2025 09:48:02
Status: Assinado eletronicamente, mediante senha de rede, pessoal e intransferível
IP: 190.***.***.**4

Rodrigo Medeiros - 284.*.***-35** - 03/10/2025 11:41:28
Status: Assinado eletronicamente, mediante senha de rede, pessoal e intransferível
IP: 191.***.***.**2

Reinaldo Pedro Correa - 813.*.***-20** - 03/10/2025 13:34:21
Status: Assinado eletronicamente, mediante senha de rede, pessoal e intransferível
IP: 170.***.***.**2

victor freire - 533.*.***-15** - 07/10/2025 06:12:26
Status: Assinado eletronicamente, mediante senha de rede, pessoal e intransferível
IP: 177.***.***.**4

PROTOCOLO DE TESTEMUNHA(S)

Eliezer Rodrigues Da Silva Benevides - 277.*.***-57** - 03/10/2025 09:01:05
Status: Assinado eletronicamente como testemunha, mediante senha de rede, pessoal e intransferível
IP: 170.***.***.**2

Cicera Mota - 620.*.***-53** - 06/10/2025 09:39:23
Status: Assinado eletronicamente como testemunha, mediante senha de rede, pessoal e intransferível
IP: 189.***.***.**6