PREGÃO ELETRÔNICO Nº 26/2025
PROCESSO DE COMPRAS Nº 848/2025
TIPO DE JULGAMENTO DA LICITAÇÃO: Menor preço por lote

A Universidade Municipal de São Caetano do Sul - USCS torna público que fará realizar a licitação na modalidade de pregão eletrônico, do tipo menor preço global por lote, conforme descrito neste Edital e seus Anexos, e em conformidade com a Lei Federal nº 14.133/2021, Lei Complementar Federal nº 123/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e 155/2016, Lei Municipal nº 4.660/2008 e portaria da Universidade USCS de número 115/2024.

UNIDADE CONTRATANTE:
Reitoria da Universidade Municipal de São Caetano do Sul – USCS

ENDEREÇO:
Avenida Goiás, 3.400, Bairro Barcelona, São Caetano do Sul - São Paulo, CEP 09550-051. telefone 55 (11) 4239-3302 e 4239-3215.

LOCAL, DATA E HORÁRIO DA SESSÃO PÚBLICA DE PROCESSAMENTO DO PREGÃO:
A sessão pública de processamento do Pregão Eletrônico será realizada no endereço eletrônico https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ mediante condições de segurança, criptografia e autenticação, em todas as suas fases.

DATA: 19/12/2025 às 9h.

PARTIICIPAÇÃO:
Ampla participação.

MODO DE DISPUTA DE LANCES:
Modo de disputa aberto.

RITO: Procedimental comum, conforme disposto no artigo 29 da Lei 14.133/2021.

O pregão em referência será conduzido por pregoeiro, devidamente designado pela autoridade superior e contará com auxílio de equipe de apoio, de acordo com regramento definido na Lei 14.133/2021 e pelas normas contidas neste edital.

1. DO OBJETO DA LICITAÇÃO

1.1. O presente pregão tem por objeto a contratação de empresa especializada para o fornecimento de infraestrutura e serviços de hospedagem em nuvem, bem como solução de segurança perimetral (Next Generation Firewall) para atendimento ao ambiente de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul, conforme condições e especificações constantes neste edital e seus anexos.

2. DAS CONDIÇÕES PARA PARTICIPAÇÃO

2.1. Poderão participar deste pregão eletrônico todos os interessados do ramo de atividade pertinente ao objeto da contratação e que atenderem a todas as exigências constantes deste edital e seus anexos.

2.1.1. O registro no Portal Eletrônico da Universidade Municipal de São Caetano do Sul, o credenciamento dos representantes que atuarão em nome da licitante no sistema de pregão eletrônico e a senha de acesso deverão ser obtidos anteriormente à abertura da sessão pública e, concedem autorização para participação em qualquer pregão eletrônico.

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

2.2. Os proponentes interessados em participar deste processo licitatório deverão retirar o edital completo e seus anexos nos endereços eletrônicos a partir dos links https://licitacao.uscs.edu.br/ ou https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/;

Nota: É importante o acesso frequente à página eletrônica da Universidade, tendo em vista que eventuais questionamentos sobre edital e os devidos esclarecimentos serão divulgados por meio eletrônico, no endereço indicado, junto ao respectivo edital, não sendo aceitas alegações de desconhecimento.

2.2.1. Os interessados em adquirir o edital pessoalmente deverão, na ocasião da aquisição, disponibilizar mídia removível (pen drive), no endereço da Rua Maceió, 177, Bairro Barcelona, São Caetano do Sul/SP, CEP 09551-030, setor de Licitações/Compras da Universidade USCS.

2.3. Estão impedidos de participar de qualquer fase do presente processo os interessados que se enquadrarem em uma ou mais das seguintes situações:

2.3.1. Organizações da Sociedade Civil de Interesse Público – OSCIP, atuando nessa condição;

2.3.2. ***Não*** poderão participar empresas estrangeiras que não funcionem no País; empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente; os interessados que se encontrem sob processo de falência, concurso de credores, dissolução, liquidação, salvo o disposto na Súmula nº 50 do Tribunal de Contas do Estado de São Paulo, bem como aqueles que tenham incorrido nas sanções dispostas no artigo 155, incisos III e IV da Lei Federal nº 14.133/2021, em substituição aos artigos da legislação revogada, dispostos na Súmula nº 51 do TCESP;

2.3.3. Não poderão participar empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

2.3.4. Pessoas físicas ou jurídicas que tenham sido declaradas inidôneas para licitar ou contratar nos termos dos §§ 4º e 5º do artigo 156, da Lei Federal nº 14.133/21. Se a punição vier a ocorrer durante o andamento desse processo, esta Administração, assegurado o direito à ampla defesa, poderá excluir a empresa do certame;

2.3.5. O impedimento de que trata o subitem 2.3.4. será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante;

2.3.6. A idoneidade dos participantes será consultada nos seguintes cadastros:

I - Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS);

II - Cadastro Nacional de Empresas Punidas (CNEP); e

III - Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa e Inelegibilidade (CNIA CNJ)

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

2.3.8. Não poderá participar empresas controladoras, controladas, nos termos da Lei nº 6.404/1976, concorrendo entre si;

2.3.9. Não poderão participar pessoas físicas ou jurídicas que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.3.10. Demais condições estabelecidas no artigo 14 da Lei Federal 14.133/2021;

2.3.11. Pessoa física ou jurídica que estejam enquadradas nas disposições do artigo 10 da Lei Federal número 9.605/1998;

2.4. Empresas reunidas em consórcio poderão participar da licitação desde que respeitados os requisitos dispostos no art.15, da Lei Federal nº 14.133/2021;

2.5. A proponente interessada em participar deste processo licitatório referenciado no lote 01, deverá declarar que detém a documentação de conformidade que é um parceiro credenciado, revendedor autorizado do fabricante, comprovando sua capacidade para oferecer e fornecer suporte aos equipamentos ofertados no formato *as a service*, bem como deverá estar apta a realizar suas implantações, assim, evitando processos de falsificação de licenciamento e até mesmo importação irregular de hardware.

2.6. Deverá ser prestada comprovação do recolhimento a título de garantia de proposta para licitar, concernente ao **lote 01**, no valor de R$ 26.681,72 (vinte e seis mil, seiscentos e oitenta e um reais e setenta e dois centavos), e para **o lote 02** o valor de R$ 16.484,99 (dezesseis mil, quatrocentos e oitenta e quatro reais e noventa e nove centavos) correspondente a 1% do valor estimado, conforme disposto no § 1º do caput do artigo 58 da Lei Federal 14.133/2021. A garantia de proposta (lotes 01 e/ou 02) poderá ser prestada optando-se por uma das modalidades de que trata o parágrafo primeiro do artigo 96 da mesma Lei.

2.6.1. Se o proponente optar pela garantia na modalidade **caução** em moeda corrente, mediante guia de recolhimento expedida pelo setor de Contabilidade e Finanças da Universidade Municipal de são Caetano do Sul, situado à Rua Maceió, 177, Bairro Barcelona São Caetano do Sul, obrigatoriamente, deverá fazê-la até 02 (dois) dias úteis anterior à abertura da sessão pública do certame.

2.6.2. O comprovante de recolhimento a título de garantia de proposta, em quaisquer das modalidades previstas no § 1º do artigo 96, deverá, obrigatoriamente, sob pena de desclassificação, integrar os documentos da proposta comercial relacionados.

2.7. *Não* poderá participar empresa que tenha sido proibida pelo Plenário do CADE de participar de licitações promovidas pela Administração Pública federal, estadual, municipal, direta e indireta, em virtude de prática de infração à ordem econômica, nos termos do artigo 38, inciso II, da Lei Federal n° 12.529/2011.

2.8. *Não* poderá participar empresa que tenha sido proibida de contratar com o Poder Público em razão de condenação por ato de improbidade administrativa, nos termos do artigo 12 da Lei Federal nº 8.429/1992.

2.9. *Não* poderá participar empresa declaradas inidônea pelo Poder Público e não reabilitadas.

2.10. *Não* poderá participar cooperativa, considerando-se que as particularidades do objeto não são atinentes ao disposto nos termos do artigo 16 da Lei Federal 14.133/2021.

2.11. Será vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente da entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

2.12. Não se admitirá oferta que não contemple a integralidade dos itens que compõe os equipamentos e/ou serviços em disputa, bem como a sua perfeita relação funcional em cada lote.

2.12.1. A licitação será composta por dois lotes, formados pelos serviços disposto no termo de referência deste edital.

2.13. A proponente que não se interessar por todos os lotes, poderá apresentar documentos de habilitação e proposta comercial apenas para aquele que pretenda disputar.

3. DA REPRESENTAÇÃO E DO CREDENCIAMENTO NO SISTEMA DE PREGÃO ELETRÔNICO

3.1. Poderão participar desta licitação, as pessoas que atenderem as exigências deste Edital.

3.2. A participação do interessado no pregão eletrônico, dar-se-á a partir da plataforma https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ na qual a licitante deverá manifestar, por meio de seu operador designado, em campo próprio do sistema, pleno conhecimento, aceitação e atendimento às exigências de habilitação previstas no edital;

3.3. O acesso ao pregão, para efeito de encaminhamento proposta de preço, lances sucessivos, documentos de habilitação e demais documentos, somente se dará mediante prévia definição de senha privativa, conforme disposto no subitem 2.1.1.;

3.4. A chave de identificação e a senha dos operadores poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado;

3.5. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo a operadora da plataforma ou ainda à USCS a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros;

3.6. O credenciamento do fornecedor junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico;

3.7. A participação no pregão estará condicionada obrigatoriamente a inscrição na plataforma, conforme descrito no subitem 3.2., antes da data e horário previsto no edital para início da sessão, e o credenciamento do licitante deverá ser requerido e acompanhado dos documentos elencados a abaixo:

3.7.1. Proposta de preços conforme disposto no modelo **Anexo II** e demais documentos obrigatórios que a integram;

3.8. O custo de operacionalização e uso do sistema ficará a cargo do licitante;

3.9. O registro no Portal de Pregão Eletrônico da Universidade Municipal de São Caetano do Sul é gratuito.

4. DA PROPOSTA COMERCIAL

4.1. O encaminhamento da proposta comercial para o sistema eletrônico pressupõe o pleno conhecimento e atendimento às exigências de classificação e habilitação previstas no edital. A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances;

4.1.1. Nos preços apresentados deverão estar inclusos todos os custos/despesas e encargos inerentes ao fornecimento dos serviços e/ou bens, correspondentes a todo o período de execução até a vigência final fixada neste edital;

4.1.2. A omissão de qualquer custo ou despesa necessária à perfeita realização do objeto será interpretada como não existente ou já incluída no preço, não podendo a empresa pleitear acréscimos. Da mesma forma, o preço apresentado deverá incluir todos os benefícios e despesas indiretas, as quais serão assim consideradas. No caso de erros aritméticos, serão considerados pelo pregoeiro, para fins de seleção e contratação, os valores retificados;

4.1.3. Serão corrigidos automaticamente quaisquer erros de soma e/ou multiplicação, bem como as divergências que porventura ocorrerem entre o preço unitário e o total do serviço, prevalecendo o valor unitário;

4.1.4. O objeto ofertado deverá atender plenamente às especificações contidas no Termo de Referência deste edital - **anexo I**. O licitante deverá fixar preço global para os serviços e/ou bens licitados em cada um dos lotes sob disputa, considerando o período de 24 meses, discriminado todos os valores unitários e totais de cada item, líquidos, fixos e irreajustáveis, em moeda nacional, expressos com duas casas decimais, desprezando-se as frações remanescentes, para a data fixada para apresentação da proposta;

4.1.5. Documento comprobatório referente ao recolhimento a título de garantia de proposta concernente ao **lote em disputa**, em quaisquer das modalidades previstas no § 1º do artigo 96 da Lei Federal 14.133/2021;

4.1.6. Não serão levadas em consideração quaisquer ofertas ou vantagens não previstas neste edital;

4.1.7. Serão desclassificadas as propostas que conflitem com as normas deste edital ou da legislação em vigor;

4.1.8. A validade da proposta será de no mínimo 60 (sessenta) dias, contados a partir da data limite para sua apresentação;

4.1.9. Quando do preenchimento da Proposta Comercial no sistema **plataforma do pregão eletrônico** da USCS, será desclassificada a proposta que identificar o licitante através da razão social, endereço, telefone ou qualquer outra informação que possibilite a identificação prévia da empresa, portanto, no curso desse edital, o proponente não deverá preencher a marca, modelo

e fabricante para os serviços de instalação e configuração, suporte e monitoramento para ambos os lotes em disputa.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS, ETAPA COMPETITIVA E JULGAMENTO DAS PROPOSTAS

5.1. A partir do horário previsto no edital e no sistema para cadastramento e encaminhamento da proposta comercial terá início a sessão pública do pregão eletrônico, quando serão divulgadas as propostas recebidas, para avaliação e aceitabilidade do pregoeiro.

5.1.1. Os licitantes deverão indicar no sistema eletrônico de licitações, antes do encaminhamento da proposta eletrônica de preços, a sua condição de microempresa ou empresa de pequeno porte para usufruirdos benefícios estabelecidos na Lei Complementar 123/2006 e suas alterações;

5.1.1.1. O licitante que não informar essa condição mencionada no subitem imediatamente acima, antes do envio da proposta perderá o direito ao tratamento diferenciado, inclusive no que concerne ao § 2º do artigo 44 da Lei Complementar 123/2006.

5.1.2. A análise das propostas pelo pregoeiro, limitar-se-á ao atendimento das condições estabelecidas neste Edital e seus anexos e à legislação vigente;

5.1.3. Para os **lotes 01 e 02**, nomeados respectivamente *(firewall as a service e data center hosting*), a licitante detentora da melhor oferta deverá apresentar imediatamente após a convocação a ser efetuada pelo agente público pregoeiro, a documentação oficial (quickspec ou datasheet) contendo as especificações técnicas dos **produtos** e **serviços** ofertados para verificação do responsável pela análise técnica, onde possam ser constatadas de forma clara e objetiva as características dos equipamentos e camadas de serviços ofertados que concretamente integrarão o contrato, sendo que tais equipamentos e serviços dispostos na proposta comercial deverão estar em conformidade com toda a especificação técnica apresentada no anexo, nomeado Termo de Referência deste edital, inclusive no que tange as certificações e homologações necessárias à consecução do projeto, como condição de julgamento da proposta comercial;

5.1.4. O sistema ordenará automaticamente as propostas classificadas pelo pregoeiro;

5.1.5. A desclassificação da proposta será fundamentada e registrada no sistema, acompanhada em tempo real por todos os participantes;

5.1.6. O licitante que tiver sua proposta desclassificada e desejar recorrer da decisão deverá observar o disposto no item 09 deste edital.

5.2. Classificadas as propostas, o agente público dará início à fase competitiva, oportunidade em que os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor;

5.2.1. O valor de redução mínima entre os lances será de 0,5% (cinco décimos por cento) e incidirá sobre o valor unitário de cada item que integra o lote em disputa, portanto, será utilizado o conceito de redução linear, cujo valor final de cada lote ajustado será apreciado em proposta readequada;

5.2.2. O licitante poderá oferecer, conforme definido no edital, valores iguais ou superiores ao menor já ofertado e registrado pelo sistema, observado o intervalo mínimo de diferença de percentuais/valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

5.3. Nos termos do Inciso I do artigo 56, da Lei Federal nº 14.133/21, será adotado o **Modo Aberto** de disputa, o qual terá etapa de lances com duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema, quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública. A prorrogação automática da etapa de lances (02 minutos) ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários. Não havendo novos lances no período de prorrogação a etapa de lances encerrar-se-á automaticamente, o pregoeiro poderá, assessorado pela equipe de apoio, se assim considerar necessário, admitir o reinício da etapa de envio de lances, na situação prevista pelo § 4º do artigo 56 da Lei Federal nº 14.133/21;

5.3.1. A situação prevista no item anterior e no § 4º do artigo 56, da Lei Federal nº 14.133/21 se destina apenas a definir as posições posteriores a proposta melhor classificada, ou seja, nessa situação não serão admitidos lances menores do que o valor da proposta melhor classificada, vez que já encerrada a etapa de lances. Os demais licitantes poderão formular outros lances, inclusive intermediários entre si;

5.3.2. O pregoeiro tem a ação de iniciar a fase de lances, depois, todo processo é automático, conforme explanado acima, desse modo, o não oferecimento de lances no prazo específico destinado a cada licitante produz a preclusão do direito de apresentá-los. Os lances apresentados em momento inadequado, antes do início do prazo específico ou após o seu término, serão considerados inválidos.

5.4. Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente que descumprir sua proposta às penalidades constantes no item 17 deste edital.

5.4.1. Excepcionalmente, o licitante poderá excluir seu último lance ofertado, **uma única vez**, no prazo de quinze segundos após o registro no sistema, caso o lance seja inconsistente, contenha erro de digitação ou seja inexequível.

5.5. Durante o transcurso da sessão pública os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais participantes.

5.6. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o pregoeiro a sua atuação no certame quando possível, sem prejuízos dos atos realizados.

5.7. Quando a desconexão persistir por tempo superior a dez minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos operadores representantes dos participantes, através de mensagem eletrônica na caixa de mensagem (chat) ou e-mail divulgando data e hora da reabertura da sessão.

5.8. Devido a impossibilidade de previsão de tempo extra, as empresas participantes deverão estimar o seu valor mínimo de lance a ser ofertado, evitando assim, cálculos de última hora, que poderão resultar em uma disputa frustrada por falta de tempo hábil.

5.9. O critério de aceitabilidade dos preços propostos pelas licitantes será o de compatibilidade com os preços praticados prelo mercado, coerentes com o objetivo ora licitado.

5.10. O sistema informará, na ordem de classificação, todas as propostas, partindo da proposta de menor preço (ou melhor proposta) imediatamente após o encerramento da etapa de lances;

5.10.1. Em caso de empate entre duas ou mais propostas, serão utilizados os critérios de desempate estabelecidos pelo artigo 60 da Lei nº 14.133/21, ressalvando-se o disposto no § 2º do artigo 44 da Lei Complementar 123/2006 que estará automaticamente assegurado no decurso desse processo licitatório.

5.11. Definido o desempate entre duas ou mais propostas, o pregoeiro poderá negociar condições mais vantajosas com o primeiro colocado;

5.11.1. Caso o primeiro colocado, mesmo após a negociação, permaneça com sua proposta acima do preço máximo definido pela Universidade USCS, a negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida.

5.12. O pregoeiro anunciará a licitante detentora da proposta ou lance de menor valor, imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão sobre a aceitação do lance de menor valor.

5.13. A escolha da melhor proposta terá como critério de julgamento o menor preço global por lote.

5.14. Após a a fase competitiva, o agente publico pregoeiro em decorrência da necessidade de avaliação técnica documental acerca dos equipamentos e/ou camadas de serviços (quickspec

ou datasheet), poderá suspender a sessão pública para execução de tal análise em relação ao proponente detentor de melhor oferta;

5.14.1. O tempo de suspensão da sessão pública, dar-se-á em decorrência da necessidade temporal para avaliação desse conteúdo pela equipe técnica.

5.15. O presente edital se submete ao disposto na Lei Complementar 123/2006 e sua posteriores alterações e aos termos da Lei Municipal nº 4660/2008 no que couber.

5.16. Serão desclassificadas as propostas:

a) apresentadas por licitante impedida de participar, nos termos do subitem 5.1.4. deste edital;

b) formuladas por licitantes participantes de cartel, conluio ou qualquer acordo conclusivo voltado a fraudar ou frustrar o caráter competitivo do certame licitatório;

c) contiverem vícios insanáveis;

d) não atendam as especificações, prazos e condições fixados neste edital;

e) apresentem preços unitários ou total simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos ou salários de mercado;

f) não tiverem sua exequibilidade demonstrada, quando exigida pelo pregoeiro.

5.17. O pregoeiro, ao final do julgamento das propostas, solicitará ao licitante mais bem classificado que envie a proposta adequada concernente ao último lance ofertado, após a negociação, se houver, **no prazo de 2 (duas) horas,** acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste edital e já apresentados, sob pena de desclassificação.

5.18. Sendo considerada aceitável a proposta de menor preço para cada lote, bem como obedecidas às exigências fixadas neste edital, o pregoeiro passará para a etapa habilitação do licitante detentor de melhor oferta que a tiver formulado, com base na documentação enviada na próprias sessão pública.

6. DA HABILITAÇÃO

6.1. Para fins de habilitação no presente Pregão o licitante vencedor deverá apresentar os documentos a seguir especificados, válidos na data de sua apresentação. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

6.1.1. Para efeito de exigência concernente aos documentos de habilitação, essa administração se pautará nos termos definidos no âmbito da Lei 14.133/2021, respeitando-se em particular, as determinações contidas nos incisos II e III do caput do artigo 63.

6.2. **Relativos à Habilitação Jurídica**:

6.2.1. Registro Comercial, para empresa individual;

6.2.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, para as sociedades empresariais, e, no caso de sociedades por ações, acompanhado dos documentos comprobatórios de eleição de seus administradores;

6.2.3. Inscrição do ato constitutivo, no caso de sociedades simples (civis), acompanhada, quando couber, de prova do registro da ata da eleição da diretoria em exercício (Registro Civil de Pessoas Jurídicas);

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

6.3. **Relativos à Regularidade Social, Fiscal e Trabalhista**:

6.3.1. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ);

6.3.2. Prova de regularidade para com a Fazenda Federal compreendendo certidão expedida pela Secretaria da Receita Federal – RFB e pela Procuradoria Geral da Fazenda Nacional – PGFN (certidão conjunta nos termos da Portaria MF 358/2014), referente a todos os tributos federais e à Dívida Ativa da União por elas administrados, abrangendo inclusive as contribuições sociais previstas nas alíneas “a” e “d” do parágrafo único do artigo 11, da Lei nº 8.212/1991;

6.3.3. Prova de regularidade para com a Fazenda estadual (relativos a dívida inscrita), consistente na apresentação de certidão que comprove regularidade fiscal ao Estado ou Distrito Federal;

6.3.4. Prova de regularidade para com a Fazenda municipal da sede da empresa licitante, consistente na apresentação de certidão de regularidade de débitos municipais mobiliários;

6.3.5. Prova da regularidade para com o Cadastro de Informativo Municipal CADIN do Município de São Caetano do Sul, emitida pelo site: https://cadin.saocaetanodosul.sp.gov.br/;

6.3.5.1. Todos os licitantes deverão apresentar o documento exigido no subitem 6.3.5. inclusive aquelas que não se encontram sediadas neste município, em cumprimento ao inciso I, do artigo 3º, da Lei 5.581/2017;

6.3.5.2. No caso de isenção ou de não incidência dos impostos devidos ao Estado e/ou Município, deverá, a licitante apresentar declaração assinada pelo representante legal, sob pena da lei;

6.3.6 Prova de Regularidade relativa ao Fundo de Garantia por Tempo de Serviço, através do Certificado de Regularidade do FGTS (CRF) ou do documento denominado "Situação de Regularidade do Empregador", com prazo de validade em vigor na data marcada para o processamento do Pregão Eletrônico;

6.3.7. Certidão de Inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas ou de Certidão Positiva de Débitos Trabalhistas com efeito de negativa, nos termos do artigo 642-A da Consolidação das Leis do Trabalho, com prazo de validade em vigor na data marcada para o processamento do Pregão eletrônico;

6.3.8. Declaração de Regularidade perante o Ministério do Trabalho no que se refere à observância do disposto no Inciso XXXIII do artigo 7º da Constituição Federal, nos termos do modelo constante, conforme modelo do **anexo IV** deste edital;

6.3.9. A licitante deverá apresentar declaração indicando que sua proposta econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas, sob pena de desclassificação conforme modelo disposto no do **anexo IX**;

6.3.10. Declaração de que cumpre as exigências de reserva de cargos para pessoas com deficiência e para reabilitados da Previdência Social previstas na Lei Federal 8.213/1991, nos termos do modelo constante do **anexo X**;

6.3.11. As licitantes que se encontram na condição de Microempresa ou Empresa de Pequeno Porte deverão nos termos da legislação fiscal, apresentar declaração de enquadramento, conforme modelo do **anexo VI** deste edital;

6.3.11.1. Para efeito da Lei Complementar Federal nº 123/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais 147/2014 e 155/2016 e, do art. 22 da Lei Municipal nº 4.660/2008, as microempresas e empresas de pequeno porte deverão apresentar toda a documentação relativa a regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição;

6.3.11.2. Havendo alguma restrição quanto à regularidade fiscal e trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, contados a partir do momento em que a licitante for declarada vencedora do certame, prorrogável por igual período, a critério da Administração, para fins de apresentação das certidões negativas ou positivas com efeito de negativas;

6.3.11.3. A licitante habilitada com pendências, deverá por ocasião da assinatura do contrato ou da retirada do instrumento equivalente, comprovar sua regularidade fiscal e trabalhista, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis.

6.3.12. Serão aceitas certidões positivas com efeito de negativas. Não constando do documento seu prazo de validade, será aceito documento emitido até 180 (cento e oitenta) dias imediatamente anteriores à data marcada para o processamento do pregão eletrônico.

6.4. **Relativos à Qualificação Econômico-Financeira**:

6.4.1. Apresentação de publicação dos dois últimos balanços patrimoniais incluindo a documentação do resultado dos exercícios 2023 e 2024. Não sendo a licitante obrigada a publicar seu balanço, deverá apresentar fotocópia legível de página do Diário Geral, onde tenha sido transcrito o balanço patrimonial, Ativo/Passivo, e a demonstração do resultado do exercício. Estes documentos deverão conter os respectivos termos de abertura e encerramento, registrados na Junta Comercial ou Cartório de Registro Civil de Pessoas Jurídicas. Esta exigência também se aplica às licitantes que optam pela Tributação Simplificada do Imposto de Renda Pessoa Jurídica ("Lucro Presumido" ou "microempresa").

6.4.2. As licitantes obrigadas ao Sistema Público de Escrituração Digital – SPED devem apresentar suas demonstrações financeiras impressas pelo sistema, devidamente validado, do ano base exigível pela lei, acompanhado dos seus respectivos Termos de Abertura e Encerramento, Demonstração do Resultado do Exercício e Recibo de Entrega.

6.4.3. A licitante que apresentar balanço patrimonial e/ou Demonstração do Resultado do Exercício em meio eletrônico deverá observar as normas de escrituração contábil em forma eletrônica pertinentes.

6.4.4. Comprovação da situação financeira da licitante desde que fique evidenciado, via demonstrativos, relativos ao balanço apresentado, o atendimento dos seguintes índices:

a) A empresa deverá apresentar os cálculos de situação financeira, baseando-se na obtenção dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), **≥ 1**(um), resultantes da aplicação das fórmulas, devidamente assinada por profissional competente (contador):

LG = (AC + RLP) / (PC + ELP)

SG = AT / (PC+ELP)

LC = AC / PC

ONDE: AC = Ativo Circulante; PC = Passivo Circulante; RLP = Realizável a Longo Prazo; ELP = Exigível a Longo Prazo e AT = Ativo Total.

b) As fórmulas deverão estar devidamente aplicadas em memorial de cálculos juntado ao balanço, devidamente assinado pelo responsável técnico (**contador**).

6.4.5. Certidão Negativa de Falência expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial expedida no domicílio da pessoa física. Não constando do documento seu prazo de validade, será aceito documento emitido até 180 (cento e oitenta) dias imediatamente anteriores à data marcada para o processamento do pregão.

6.5. **Relativos à Qualificação Técnica**:

6.5.1. Comprovação de aptidão para o fornecimento do objeto do presente edital, estando de acordo com as características, quantidades e prazos compatíveis. A comprovação deverá ser feita por meio de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, competentes para tanto, sendo que os quantitativos mínimos de prova de fornecimento similares obedecerão ao percentual de 50% (cinquenta por cento), nos termos do artigo do artigo 67, § 2º, da Lei Federal 14.133/2021. Somente serão considerados válidos atestados com timbre da entidade expedidora e com identificação do nome completo. O atestado deverá ser datado e assinado por pessoa física identificada pelo seu nome e cargo exercido na entidade, bem como dados para eventual contato, estando as informações sujeitas à conferência pelo pregoeiro.

6.5.1.1. O(s) quantitativo(s), quando não mencionado(s) no(s) atestado(s), poderá(ão) ser comprovado(s) por quaisquer documentos, tais como: contrato(s), nota(s) fiscal(is) ou outro(s) documento(s) equivalente(s);

6.5.2. Para o **lote 01**, o licitante deverá **Declarar** na forma do **Anexo XII**, que detém *status de parceiro credenciado do fabricante,* como condição de fornecedor na área de serviço de segurança de redes, ou, que é revendedor autorizado do fabricante, indicando sua capacidade para oferecer e fornecer suporte aos equipamentos ofertados *as a service*, bem como deverá estar apto a realizar suas implantações.

6.6. **Relativo à capacitação Profissional**

6.6.1. A licitante deverá indicar em declaração (**Anexo XI**), que dispõe de pelo menos um profissional com qualificação técnica mínima compatível com as exigências de cunho técnico/tecnológicos para suportar a implantação, configuração, suporte técnico e manutenção, bem como as atividades laborais vinculadas à segurança de rede e monitoramento NOC, considerando-se que esse profissional estará à frente da equipe de pessoal necessário à prestação dos serviços concernentes ao objeto do certame, respeitando-se as particularidades inerentes ao escopo de contratação para cada lote em disputa.

6.6.2. A licitante deverá apresentar, no ato de celebração do contrato, a comprovação de certificação técnica necessária do profissional que comandará a equipe de trabalho designada para consecução do projeto, consoante ao disposto no subitem 6.6.1., sob pena de, em não apresentando, sujeitar-se às penalidades dispostas no item 17 deste edital.

6.7. **Outras exigências de Qualificação**:

6.7.1. Declaração de atendimento às normas relativas à saúde e segurança no trabalho, em virtude das disposições do parágrafo único, artigo 117 da Constituição do Estado de São Paulo, nos termos do modelo constante do constante do **Anexo VII** deste edital;

6.7.2. Declaração de que cumpre o pleno atendimento aos requisitos de habilitação nos termos do modelo constante no **Anexo V** deste edital;

6.7.3. Declaração de atendimento às condições gerais de privacidade, nos termos da Lei Federal 13.709/2018 – LGPD, descritos no modelo registrado sob a forma do **Anexo VIII** - “Declaração de Condições Gerais de Privacidade e Proteção de Dados de Pessoas.

7. DISPOSIÇÕES GERAIS DA HABILITAÇÃO

7.1. O licitante poderá suprir eventuais omissões ou sanear falhas relativas ao cumprimento dos requisitos e condições de habilitação estabelecidos neste Edital mediante a apresentação de documentos, preferencialmente por correio eletrônico a ser fornecido pelo pregoeiro no chat do sistema, desde que os envie no curso da própria sessão pública e antes de ser proferida decisão sobre a habilitação;

7.2. A verificação será certificada pelo pregoeiro e deverá ser anexada aos autos os documentos passíveis de obtenção por meio eletrônico, salvo impossibilidade devidamente justificada;

7.3. A administração não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos no momento da verificação, ressalvada a indisponibilidade de seus próprios meios. Na hipótese de ocorrerem essas indisponibilidades e/ou não sendo supridas ou saneadas as eventuais omissões ou falhas, a licitante será inabilitada, mediante decisão motivada;

7.4. Não serão aceitos documentos autenticados digitalmente pelo **Cartório Azevedo Bastos**, considerando-se a impossibilidade de consultar a autenticidade das autenticações, conforme comunicado disponibilizado no site do referido Cartório;

7.4.1. *“Em razão de intervenção determinada pela Conselheira Jane Granzoto Torres da Silva, do Conselho Nacional de Justiça, o 1º Registro Civil de Pessoas Naturais de João Pessoa está sob a responsabilidade de Sidnei da Silva Perfeito. Também em razão da intervenção, estão suspensos quaisquer serviços de autenticação digital”.*

7.5. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos nos termos da Medida Provisória nº 2.200-2, ou ainda do artigo 5º da Lei Federal 14.063/2020, serão recebidos e presumidos verdadeiros em relação

aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel;

7.6. Caso a licitante provisoriamente vencedora com o menor preço venha a desatender as exigências para a habilitação, o pregoeiro examinará a melhor oferta subsequente e negociará com o seu autor, decidindo sobre sua aceitabilidade e, em caso positivo, verificando as condições de habilitação e assim sucessivamente, até a apuração de uma oferta aceitável cuja autoria atenda aos requisitos de habilitação, caso em que será declarada vencedor.

8. DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO E PEDIDO DE ESCLARECIMENTO AO EDITAL

8.1. Qualquer pessoa é parte legítima para impugnar o edital de licitação por irregularidade na aplicação da Lei, ou pedir esclarecimentos devendo protocolar o pedido até 3 (três) dias úteis antes da data de abertura do certame, ou seja, **até às 23:59 horas do dia 15/12/2025**, no endereço da a Rua Maceió, 177, Bairro Barcelona, São Caetano do Sul - São Paulo, CEP 09551-030 ou, preferencialmente por meio da inserção na plataforma do pregão eletrônico https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ , ou ainda a partir do envio por e-mail no endereço licitacao@online.uscs.edu.br quando se tratar de pedido de esclarecimentos/questionamentos.

8.1.1. Concernente à impugnação, o seu devido conhecimento/recebimento se dará somente com o ingresso dos documentos que configure competência e poderes para exercer tal ação, juntamente com o documento sob a forma de peça impugnatória. Neste sentido, ainda não serão conhecidas as impugnações apresentadas fora do prazo legal

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

8.3. Todas as solicitações de esclarecimento, bem como suas respostas serão numeradas sequencialmente e serão consideradas como aditamentos a este instrumento convocatório, sendo juntadas ao respectivo processo licitatório.

8.4. Caberá a autoridade competente receber, examinar e decidir as impugnações (signatário do edital) e, ao pregoeiro caberá decidir sobre as solicitações de esclarecimento ao edital e aos anexos, além de poder requisitar subsídios formais aos responsáveis pela elaboração desses documentos, bem como contar com o auxílio técnico e/ou jurídico.

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

8.5. Acolhida a impugnação ou os esclarecimentos apresentados em face do Edital e a modificação consubstanciada na decisão, NÂO comprometer os aspectos de formulação da proposta por parte dos proponentes, ou ainda não se traduzam em prejuízo no prazo de apresentação dos documentos relativos à sua participação no certame, a data original da sessão do pregão eletrônico será resguardada, caso contrário, será designada nova data para a realização do certame (§ 1º, art. 55, Lei nº 14.133/21).

8.6. Em caso de não solicitação, pelas empresas licitantes, de esclarecimentos ou informações, pressupõe-se que os elementos fornecidos são suficientemente claros e precisos, não cabendo, posteriormente, o direito a qualquer reclamação.

8.7. Não serão aceitas consultas, reclamações, impugnações ou questionamentos efetivados por meio de ligação telefônica ou consulta verbal.

9. DOS RECURSOS ADMINISTRATIVOS

9.1 Declarada vencedora, o pregoeiro informará às licitantes por meio de mensagem lançada no sistema, da qual poderão manifestar sua intenção de interpor recurso, que deverá ser realizada por meio eletrônico, utilizando exclusivamente o campo próprio disponibilizado no sistema de pregão no prazo de 10 (dez) minutos.

9.2. Havendo manifestação da intenção de interposição de recurso, será concedido o prazo de 03 (três) dias úteis para apresentação das razões recursais, ficando as demais licitantes, desde

logo, convocados para apresentar contrarrazões em igual número de dias úteis (03), que contarão a partir do término do prazo do recorrente, sendo-lhes assegurada vista imediata aos autos do processo.

9.3. A formalização dos recursos, observados os prazos legais, será dirigida ao pregoeiro nos termos do art. 165, § 1º, da Lei 14.133/2021, e será efetivada por meio de documento com identificação do Processo e número do Pregão eletrônico **devendo ser redigido ou anexado em campo específico do sistema**, sob pena de decadência do direito de recorrer.

9.4. A falta de manifestação imediata da licitante, bem como a não apresentação das razões recursais no prazo estabelecido no item 9.2., importará na decadência do direito de recorrer da decisão.

9.5. O recurso contra decisão do pregoeiro terá efeito suspensivo.

9.6. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

9.7. Não serão conhecidos os recursos interpostos após os respectivos prazos legais, bem como os encaminhados por endereçamento postal, correio eletrônico (e-mail) ou em desacordo com o estabelecido nos itens 9.2. e 9.3. deste edital.

9.8. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade superior adjudicará e homologará o processo licitatório e determinará a convocação das adjudicadas para a assinatura do contrato e retirada da ordem de início de serviços.

10. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

10.1. O objeto da licitação será adjudicado e homologado ao licitante declarado vencedor, por ato da Autoridade Superior da Universidade Municipal de São Caetano do Sul.

11. DA CONTRATAÇÃO

11.1. O instrumento contratual resultante desse processo licitatório deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial

11.2. Após a homologação do certame, o proponente vencedor será convocado para assinar o instrumento contratual no prazo de 05 (cinco) dias úteis, em conformidade com a minuta apresentada na forma do anexo XIII, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas na Lei 14.133/2021, no edital e outras legislações aplicáveis;

11.2.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificado e, desde que aceito pela contratante;

11.3. Na hipótese de o vencedor da licitação não assinar o contrato ou manifestar a recusa no recebimento da nota de empenho, no prazo e nas condições estabelecidas, sem prejuízo da aplicação das sanções previstas na Lei 14.133/2021, no edital e em outras legislações aplicáveis, será facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para apresentar os documentos de habilitação nos termos definidos neste edital para celebrar a contratação, nas condições definidas em proposta pelo licitante vencedor;

11.4. Antes de formalizar a contratação ou prorrogar o prazo de vigência do contrato, a Administração deverá além de verificar a regularidade fiscal e trabalhista do contratado, consultar o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), Cadastro Nacional de Empresas Punidas (CNEP) e o Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa e Inelegibilidade (CNIA CNJ), emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo;

11.4.1. Se o adjudicatário incorrer nas penalidades do artigo 156, incisos III e IV da Lei 14.133/21, ficará impedido de contratar com a Administração;

11.5. Se, por ocasião da formalização do contrato, a prova de regularidade para com a Fazenda Federal (através da Certidão Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União nos termos da Portaria MF 358/2014 – unificada com a Certidão de

Regularidade de Débitos relativos às Contribuições Previdenciárias e às de Terceiros) e a prova de regularidade para com o Fundo de Garantia por Tempo de Serviço, através do Certificado de Regularidade do FGTS (CRF) ou do documento denominado "Situação de Regularidade do Empregador", estiverem com os prazos de validade vencidos, a USCS verificará a situação por meio eletrônico hábil de informações, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios, salvo impossibilidade devidamente justificada;

11.5.1. Havendo a impossibilidade da obtenção dos documentos por meio eletrônico, será a adjudicatária notificada para que providencie o envio da documentação sob pena de decair o direito ao fornecimento, sem prejuízo das sanções previstas no artigo 156 da Lei Federal 14.133/21;

11.6. Até a assinatura do instrumento contratual a vencedora poderá ser inabilitada se a Universidade USCS tiver conhecimento de fato desabonador à sua habilitação, conhecido após o julgamento, nos termos da Lei de Licitações.

11.7. Quando do recebimento do instrumento contratual, o adjudicatário deverá também assinar o termo de Ciência e Notificação;

11.8. A Universidade Municipal de São Caetano do Sul providenciará a publicação do instrumento contratual, resultante deste processo licitatório no Portal Nacional de Contratações Públicas (PNCP) e de seus eventuais termos aditivos na forma prevista no artigo 94 da Lei 14.133/2021.

12. DOS PRAZOS PARA ENTREGA E EXECUÇÃO DOS SERVIÇOS

12.1. A Contratada deverá cumprir os seguintes prazos para a perfeita execução do instrumento contratual a ser celebrado com a Universidade Municipal de São Caetano do Sul:

12.1.1. A Contratada deverá cumprir o prazo estipulado de até 60 dias para fornecimento dos equipamentos de firewall *as a service*, licenciamento, bem como instalação e configuração relativas ao **lote 01**, a contar da aprovação do projeto executivo pelo gestor do contrato;

12.1.2. Em relação ao **lote 02**, a contratada terá prazo de 60 dias para migração das aplicações e base de dados legado, instalação e configuração dos equipamentos na nova estrutura computacional in cloud, computados a partir da aprovação do projeto executivo pelo gestor do contrato;

12.1.3. A empresa deverá elaborar plano de implementação junto a Universidade USCS, nos termos dos subitens 1.11.10 e 2.9.10. aportados ao TR do edital, respectivamente para os lotes 01 e 02, compondo o documento nomeado “Projeto Executivo” em até 10 dias úteis, computados a partir do dia seguinte ao envio da ordem de serviços, cujo escopo remete às especificações contidas no Termo de Referência do edital.

12.2. Caso a ordem de serviço seja enviada por correspondência eletrônica, o prazo para entrega dos equipamentos *as a service*, migração das aplicações e base de dados legado, instalação e configuração da solução para qualquer dos lotes contratados, independente do recebimento, inicia-se 24 (vinte e quatro) horas após sua expedição, ressaltando-se que o prazo deve iniciar em dia útil.

12.3. Concluído a fase de estruturação, que contempla a disponibilização física de equipamentos *as a service*, migração das aplicações e bases de dados legado, com escopo definido a partir das especificações contidas no termo de referência do edital, acompanhados de sua respectiva instalação e configuração, distintamente para ambos os lotes, o gestor do contrato designado pela USCS terá o prazo máximo de até 5(cinco) dias para conferência e emissão do **TERMO DE ACEITAÇÃO**.

12.3.1. Em particular, no que concerne ao lote 01, a implantação dos equipamentos *as a service*, bem como os serviços de instalação e configuração, dar-se-ão de modo parcial, de acordo com o cronograma a ser definido entre a Contratada e a gestão do instrumento de contrato da Universidade USCS. Portanto, o **termo de aceitação** e consequentemente pagamento por essa etapa de infraestrutura será paulatino, do mesmo modo, a ativação dos serviços decorrentes de tal implantação (suporte técnico 24x7 e monitoramento NOC).

12.3.2. O cronograma de execução, notadamente relativo ao lote 01, deverá indicar de modo percentual a distribuição e execução dos serviços, considerando-se o dimensionamento e as respectivas unidades da Universidade USCS que integram o projeto, estabelecido no termo de referência do edital (item 1 “a”).

12.4. Quanto ao início dos serviços de suporte técnico, serviços de monitoramento NOC no formato 24x7(mensal para ambos os lotes), bem como serviço de segurança de rede lote 01 e serviço computacional in cloud lote 02, serão computados para efeito de pagamento na data constante do termo de aceitação emitida pela gestão do instrumento de contrato da Universidade USCS, respeitando-se a condição (*pró-rata - no sentido de proporcionalidade*) disposta no subitem 12.3. e seguintes para o primeiro pagamento, caso não se inicie no primeiro dia do mês.

12.4.1. Para efeito de pagamento relativa aos serviços descritos no subitem imediatamente anterior, deverá ser considerado o escopo de fornecimento e a distinção em cada um dos lotes contratados.

***Importante*:** Reunião inicial para definição de cronograma do projeto - após o envio da ordem de serviços, será agendada uma reunião no prazo de até 05 dias pelo gestor designado para o acompanhamento do contrato, onde será elaborado o **Cronograma** de execução de serviços para que sejam cumpridos os prazos supracitados. Dessa reunião será lavrada em Ata circunstanciada que deverá ser acostada ao processo de compras.

13. DA VIGÊNCIA DO CONTRATO

13.1. A Universidade Municipal de São Caetano do Sul firmará contrato resultante deste processo licitatório para os serviços de suporte técnico, monitoramento (NOC) e segurança de rede (firewall *as a service*), consoante lote 01, assim como serviço mensal de suporte técnico, manutenção e monitoramento (NOC) referente a estrutura computacional em Data Center e Hosting, registrados nos termos definidos para o lote 02, por prazo de 24 (vinte e quatro) meses consecutivos e ininterruptos, contados a partir do recebimento da ordem de serviços, conforme disposto no subitem 12.2. podendo ser prorrogado por igual período, de comum acordo, desde que devidamente justificado e manifestado com antecedência mínima de 60 (sessenta) dias antes do seu término, estendendo-se até o limite máximo de 120 meses, nos termos do artigo 107, da Lei Federal 14.133/2021.

13.2. No caso de prorrogação será lavrado o respectivo termo.

14. DO FATURAMENTO E DO PAGAMENTO

14.1. A empresa contratada, quando da disponibilização dos equipamentos e execução dos serviços migração das aplicações e base de dados legado, instalação e configuração conforme descritos no termo de referência para os respectivos lotes distintos, deverá comunicar por escrito o evento e emitir as respectivas notas fiscais, encaminhando-as ao fiscalizador técnico designado para o contrato para averiguação e emissão dos respectivos termos e posterior liberação dos pagamentos correspondentes.

14.1.1. Para efeito de pagamento particularmente referente ao lote 01, obrigatoriamente, deverá ser respeitado a condição definida no subitem 12.3.1. deste edital.

14.1.2. O pagamento distinto para cada lote será efetuado à Contratada em uma única parcela, no prazo até 10 (dez) dias uteis, contados do primeiro dia seguinte ao recebimento do Termo de Aceitação juntamente com a documentação fiscal completa (nota fiscal e demais documentos exigíveis), pelo setor de contas a pagar da Universidade USCS.

14.2. **Faturamento mensal**

14.2.1. A empresa Contratada emitirá uma nota fiscal mensal discriminando os serviços de segurança firewall *as a service* (tipo 1, 2 e 3); suporte técnico com atendimento local e remoto; serviço de monitoramento (NOC), referente ao lote 01 **ou**, serviço de data center hosting; serviço de suporte técnico; serviço de monitoramento (NOC) referente ao lote 02, no último dia útil do mês de prestação desses serviços, encaminhando-a ao gestor/fiscalizador do contrato, que deverá, no máximo no próximo dia útil efetuar a conferência, liberação e encaminhamento ao setor de contas a pagar da Universidade USCS.

14.2.2. O pagamento do serviço mensal será efetuado na 2ª (segunda) terça-feira do mês subsequente ao início dos serviços, desde que a nota fiscal e **Termo de liberação de pagamento** emitido pelo gestor/fiscalizador do contrato seja encaminhado ao setor de contas a pagar da USCS no prazo mencionado no subitem 14.2.1.

14.2.3. Para efeito de pagamento no primeiro período (mês), considerando-se a distinção dos lotes, dar-se-á embasado no termo de aceite do Gestor do instrumento contratual e, será proporcional ao número de dias efetivos da prestação dos serviços em cada lote contratado.

14.3. Caso o término da contagem aconteça em dias sem expediente bancário, o pagamento ocorrerá no primeiro dia útil imediatamente subsequente.

14.4. A Universidade USCS poderá exigir a comprovação de quitação das obrigações trabalhistas vencidas relativas ao contrato, de acordo com disposto no § 3º do artigo 121 da Lei 14.133/2021 como condição para liberação de pagamento.

14.5. Havendo divergência ou erro na emissão da documentação fiscal, será interrompida a contagem do prazo para fins de pagamento, sendo iniciada contagem somente após a regularização da documentação fiscal.

14.5.1. Constatado a situação de irregularidade, o contratado será notificado formalmente, para que, no prazo de até 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da USCS.

14.6. A permanência da condição de irregularidade, sem a devida justificativa ou com justificativa não aceita pela USCS, poderá culminar em rescisão contratual, sem prejuízo da apuração de responsabilidade e da aplicação de penalidades fixadas no item 17 deste edital, observado o contraditório e a ampla defesa.

14.6.1. Eventualmente, em caso de atraso pela USCS no pagamento pelos serviços executados, desde que a empresa contratada não tenha concorrido de alguma forma para tanto, o valor devido deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para opagamento até a data do efetivo pagamento, à taxa de 6% (seis por cento) ao ano, aplicando-se a seguinte fórmula:

EM = I x N x VP

EM = Encargos Moratórios a serem acrescidos ao valor originalmente devido

I = Índice de atualização financeira, calculado segundo a fórmula:

I = (6 / 100) / 365

N = Número de dias entre a data limite prevista para o pagamento e a data do efetivo pagamento

VP = Valor atualizado da parcela em atraso.

14.6.1.1. Em caso de atraso superior a 30 dias do vencimento, o valor principal será atualizado monetariamente pelo índice IPCA do último mês, anterior à data limite, divulgado pelo IBGE.

14.6.1.2. Para efeito de aplicação dos itens imediatamente acima, a empresa contratada deverá apresentar solicitação expressa e formal, ocasião em que se realizará a análise e negociação com a USCS.

14.7. A Universidade USCS emitirá ordem de pagamento a crédito em conta bancária em nome do credor, que poderá ser indicada na "Proposta Comercial", ficando terminantemente vedada a negociação da duplicata mercantil na rede bancária ou com terceiros.

14.8. Independente do percentual de tributo inserido na planilha que define a proposta comercial, quando houver, serão retidos na fonte, na realização do pagamento, os percentuais estabelecidos na legislação vigente.

15. DAS RESPONSABILIDADES E OBRIGAÇÕES DA CONTRATADA

15.1. No cumprimento deste edital, a licitante obrigar-se-á:

15.1.1. Executar o objeto do certame sob sua inteira responsabilidade, rigorosamente de acordo com as especificações contidas nos anexos I e II. É salutar reafirmar que a Contratante não aceitará fornecimento de serviço ou equipamentos físicos e/ou virtuais ou ainda softwares e garantias, diferentes daqueles dispostos no Termo de Referência deste edital.

15.1.2. Manter durante a execução do contrato, em compatibilidade com as obrigações assumidas todas as condições de habilitação e qualificação exigidas na licitação.

15.1.3. Responsabilizar pelo fornecimento dos bens e execução dos serviços objeto da licitação, cabendo ao seu representante na condição de preposto acompanhar o cumprimento rigoroso dos prazos, organização de reuniões, entrega de documentos, elaboração de relatórios de acompanhamento e quaisquer atividades pertinentes à execução dos serviços.

15.1.4. Registrar as ocorrências havidas durante a execução do objeto dando ciência a Universidade Municipal de São Caetano do Sul, respondendo integralmente por sua omissão.

15.1.5. Manter durante a execução do objeto, todas as condições de habilitação e qualificação exigidas no processo licitatório.

15.1.6. Prestar os serviços sempre por pessoal qualificado, respondendo perante a USCS e terceiros por todos os ônus, encargos, perdas e/ou danos porventura resultantes da execução do objeto da prestação de serviços.

15.1.7. Providenciar e custear pessoal habilitado em quantidade necessária para a execução dos serviços até o cumprimento integral do contrato.

15.1.8. Providenciar e custear os recursos computacionais (hardware, software e/ou estrutura computacional em hosting), quando couber, utilizados por sua equipe de suporte técnico, monitoramento NOC e de segurança de rede no desempenho de suas funções exigidas via celebração de contrato, respeitando-se as particularidades em cada lote contratado.

15.1.9. Manter equipe de profissionais treinados nas melhores práticas e tecnologias existentes no mercado de cibersegurança.

15.1.10. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer dados ou informação de que tenha tomado ciência em razão da execução dos serviços discriminados neste instrumento, sem o consentimento, prévio e formal da Universidade USCS.

15.1.11. A Universidade USCS não assumirá nenhuma responsabilidade pelo pagamento de impostos e outros encargos que competirem à Contratada, nem se obrigará a fazer a essa qualquer restituição ou reembolso de quantias ou acessórios que a mesma despender com esses pagamentos.

15.1.12. A licitante contratada poderá realizar subcontratação parcial do objeto (atividades relacionadas a etapa de fornecimento de equipamentos e sua infraestrutura...), desde que tal subcontratação não diga respeito à atividade fim do objeto do certame, conforme disposto no artigo 122 da Lei 14.133/2021, contudo, sua efetiva realização deverá ser devidamente justificada e precedida expressamente de autorização da Universidade Municipal de São Caetano do Sul.

15.1.13. A subcontratação dos serviços, inclusive a aquisição dos equipamentos, será de inteira responsabilidade da licitante que será contratada e deverá seguir as condições e especificações delimitadas para o objeto no termo de referência deste edital.

15.1.14. Para efeito da respectiva subcontratação, a licitante apresentará à administração documentação que comprove capacitação técnica do subcontratado, que deverá ser avaliada e acostada aos autos do processo.

16. DA FISCALIZAÇÃO E SUPERVISÃO

16.1. Não obstante ser a Contratada a única e exclusiva responsável, inclusive perante terceiros, pela execução do objeto do contrato, reserva-se à Universidade Municipal de São Caetano do Sul o direito de, sem que de qualquer forma restrinja a plenitude da responsabilidade da Contratada, exercer a mais ampla fiscalização para a consecução do objeto.

17. DAS SANÇÕES ADMINISTRATIVAS E PENALIDADES

17.1. Comete infração administrativa, nos termos da Lei Federal 14.133/2021, a proponente vencedora do certame e/ou contratada que der causa à inexecução parcial ou total do contrato; ensejar o retardamento da execução do instrumento; apresentar documentação falsa ou praticar ato fraudulento durante a execução do contrato; comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; praticar ato lesivo previsto no artigo 5º da Lei Federal 12.846/2013.

17.1.1. As empresas que cometerem as infrações dispostas no item 17.1, estarão sujeitas a aplicação de advertência formal, impedimento de licitar e contratar com a administração pública, ser declarada inidônea para licitar e contratar, além da aplicação de multas reparatórias e/ou moratórias, conforme o caso.

17.1.2. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Universidade USCS, bem como não impede essa administração de se utilizar cumulativamente da aplicação das sanções com as multas previstas.

17.2. A recusa injustificada da adjudicatária em aceitar ou retirar o termo de contrato, no prazo e nas condições estabelecidas caracterizará descumprimento total da obrigação assumida, sujeitando-o a juízo da Administração, nos termos, inclusive, da legislação municipal:

a) À multa de 30% (trinta por cento) sobre o valor do contrato;

b) Ao pagamento correspondente à diferença de preço decorrente de nova licitação ou contratação, para o mesmo fim;

17.2.1. O disposto no subitem 17.2. não se aplicará aos licitantes remanescentes quando convocados nos termos do subitem 11.3. deste edital.

17.3. Pela inexecução total do contrato, será aplicada à Contratada a multa de 30% (trinta por cento) sobre o valor total do ajuste;

17.4. Pela inexecução parcial do contrato, será aplicada à Contratada a multa de 20% (vinte por cento) sobre o valor da obrigação não cumprida.

17.5. Pelo atraso injustificado a Contratada incorrerá em multa diária de 0,5% (cinco décimos por cento) sobre o valor do contrato, excluída, quando for o caso, parcela correspondente aos impostos incidentes, quando destacados no documento fiscal, sendo que a aplicação da multa terá início no primeiro dia seguinte ao término do prazo contratual do serviço.

17.5.1. Os atrasos injustificados superiores a 30 (trinta) dias corridos serão obrigatoriamente considerados inexecução total ou parcial, estando a Contratada sujeita as sanções previstas nos subitens 17.3 ou 17.4.

17.6. Além das multas e das penalidades aqui contidas, poderão ser aplicadas à Contratada, sanções decorrentes do não cumprimento das condições estabelecidas pelo ***Service Level Agreement*** que integra o Termo de Referência do edital, itens 1.14 e 2.13., conforme verificação e enquadramento do Gestor do instrumento de contrato designado pela USCS.

17.7. As multas a que aludem os subitens anteriores não impedem que a Administração rescinda unilateralmente o contrato e aplique outras sanções previstas nas Leis Federais e Municipais, a saber:

17.7.1. Advertência, por escrito, no caso de pequenas irregularidades.

17.7.1.1. A sanção de advertência poderá ser aplicada nos seguintes casos:

I. Descumprimento das determinações necessárias à regularização das faltas ou defeitos observados na prestação dos serviços;

II. Outras ocorrências que possam acarretar transtornos no desenvolvimento dos serviços da USCS, desde que não caiba a aplicação de sanção mais grave.

17.7.2. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração, pelo prazo de até três anos, quando da inexecução contratual sobrevier prejuízo para a Administração;

17.7.2.1. A penalidade de suspensão será cabível quando o licitante participar do certame e for verificada a existência de fatos que o impeçam de contratar com a Administração Pública. Caberá ainda a suspensão quando a licitante, por descumprimento de cláusula contratual tenha causado transtornos no desenvolvimento dos serviços da USCS.

17.7.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação.

17.7.3.1. Se o licitante deixar de entregar a documentação ou apresenta-la falsamente, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará, pelo prazo de até cinco anos, impedido de contratar com a Administração Pública, sem prejuízo das multas previstas no edital e das demais cominações legais.

17.7.4. Verificado que a obrigação foi cumprida com atraso injustificado caracterizando a inexecução parcial, a USCS poderá reter preventivamente, o valor da multa dos eventuais créditos que a Contratada tenha direito, até a decisão definitiva, assegurada a ampla defesa.

17.7.4.1. Se a USCS decidir pela não aplicação da multa, o valor retido será devolvido à Contratada.

17.8. Os atos previstos como infrações administrativas na Lei Federal nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

17.9. Independentemente das sanções retro, a Contratada ficará sujeita ainda, à composição das perdas e danos causados à Administração, decorrentes de sua inadimplência, bem como arcará com a correspondente diferença de preços verificada em nova contratação, na hipótese de os demais classificados não aceitarem a contratação pelos mesmos preços e prazos fixados pelo inadimplente.

17.10. A personalidade jurídica da empresa vencedora poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Edital para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios

com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a empresa vencedora.

17.11. É assegurada nos termos legais os prazos para exercício do direito da ampla defesa e do contraditório, na aplicação das sanções previstas no escopo dos artigos 155 a 162 da Lei 14.133/2021, conforme o caso.

18. DO REAJUSTE DE PREÇOS

18.1. Os valores constantes da proposta e expressos em reais para prestação dos serviços de suporte técnico 24x7, manutenção, monitoramento NOC, serviço de segurança firewall *as a service(tipo 1, 2 e 3)* referentes ao lote 01, bem como o serviço de hospedagem da estrutura computacional em hosting, serviço de suporte técnico 24x7, manutenção e monitoramento NOC vinculados ao lote 02, poderão sofrer reajustes somente após o interregno de 12 meses, contados nos termos previstos no subitem 12.3. e seguintes deste edital.

18.2. Na hipótese de manutenção do contrato, transcorridos os primeiros 12 meses, de acordo com a especificidade dos serviços elencados no item 18.1., poderão ser reajustados partir do 13º (décimo terceiro) mês, de acordo com a variação do Índice Nacional de Preços ao Consumidor Amplo – IPCA/IBGE, conforme legislação em vigor ou por outro índice que venha substituí-lo.

18.3. O reajuste poderá ser concedido mediante expressa solicitação da Contratada, para análise e negociação com a USCS, e terá incidência de pagamento respeitando-se as condições e períodos estabelecidos no item 18.1.

18.4. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, aquele que vier a ser determinado pela legislação então em vigor.

19. DA GESTÃO DO CONTRATO

19.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei 14.133/2021, e cada parte responderá pelas consequências de sua inexecução.

19.2. O agente público designado para assumir a função de Gestor do instrumento contratual resultante deste processo licitatório será o responsável pela Diretoria de Tecnologia da Informação e Inovação, cujas atribuições lhes permitirá ainda estabelecer os fiscalizadores técnicos. Os designados serão responsáveis pelo acompanhamento e execução do termo contratual objeto do presente certame, procedendo, de acordo com suas competências, ao registro das ocorrências e adotando as providências necessárias ao fiel cumprimento do ajuste, bem como, responsabilizar-se-ão pela vigência, com o consequente controle dos prazos de início e término contratual, eventual prorrogação, aditamentos e instauração de novo processo de licitação quando couber.

19.3. Os fiscais técnicos do contrato anotarão para efeito de histórico de gerenciamento, todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. Identificada quaisquer irregularidades, este emitirá notificação, indicando o prazo para correção em sua execução.

19.4. Os fiscais técnicos comunicarão ao gestor desse instrumento, em prazo não inferior a 60 (sessenta) dias do término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

19.5. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal daliquidação e do pagamento da despesa.

19.6. O gestor do contrato deverá coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

19.7. O gestor tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido por comissão, ou, pelo departamento competente para tal, em conformidade ao disposto no artigo 158 da Lei 14.133/2021.

19.8. O gestor deverá elaborar relatório final contendo informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades relativas à administração e execução contratual.

20. DA DOTAÇÃO ORÇAMENTÁRIA

20.1. As despesas decorrentes da contratação, objeto deste processo licitatório, correrão à conta dos recursos consignados no orçamento da Contratante, em conformidade com o disposto no parágrafo 2º do artigo 12 da Lei nº. 10.320, de 16 de dezembro de 1968, de acordo com a dotação orçamentária.

20.2. No tocante à classificação das despesas Orçamentárias pertinentes a este certame é conjecturada a de número 12.364.1500.2.100.3.3.90.40.00.

21. DA GARANTIA CONTRATUAL

21.1. A licitante declarada vencedora, em até 10(dez) dias úteis contados da assinatura do contrato, deverá fazer prova de recolhimento, a título de Garantia de Execução do Contrato, equivalente a 5% (cinco por cento) do valor total pactuado, com vencimento para 60 (sessenta) dias após a data da entrega final dos serviços, correspondente a data da última parcela a ser paga pela Universidade Municipal de São Caetano do Sul, cabendo à Contratada optar por quaisquer modalidades assecuratórias previstas no parágrafo 1º do artigo 96 da Lei Federal 14.133/2021.

21.1.1. A garantia quando prestada nas modalidades fiança bancária e seguro garantia, deverá prever a cobertura de indenizações decorrentes de responsabilização da **Tomadora** dos serviços por obrigações assumidas pela Contratada, inclusive às concernentes aos encargos trabalhistas, previdenciários, fiscais e comerciais, nos termo deste contrato.

21.1.2. Na hipótese de o contratado optar pela modalidade de garantia inscrita no inciso II do parágrafo 1º do artigo 96 (Lei 14.133/2021), o prazo para prestação de garantia será assegurado nos termos do § 3º do mesmo artigo da mesma Lei, contudo, sua aplicação dar-se-á subsidiariamente ao contido no item 21.1 deste edital .

21.2. Na hipótese de evidenciar qualquer impropriedade ou incorporação, a Contratante exigirá sua regularização ou substituição no prazo de 5(cinco) dias úteis da data de intimação.

21.3. A falta de atendimento à convocação para regularização ou substituição da garantia na forma e prazo especificado no item 21.2. acima, sujeitará a Contratada às seguintes consequências:

a) Retenção dos pagamentos que lhe sejam devidos, para recomposição da garantia contratual, na modalidade caução em dinheiro; ou

b) Caracterização de inexecução contratual, ensejando a consequente aplicação de penalidade prevista na item 17 deste documento e, ainda, a rescisão do ajuste com fundamento nos incisos do artigo 155 da Lei Federal nº 14.133/2021.

21.3.1. Caberá a Contratante decidir motivadamente entre a retenção de pagamentos para recomposição da garantia contratual ou a caracterização da inexecução contratual.

21.4. A correção monetária da garantia prestada na forma de caução em dinheiro será calculada com base na variação do índice IPCA/IBGE e, no caso de utilização de cheque, a data inicial da correção será a do crédito bancário.

22. DA GARANTIA DOS EQUIPAMENTOS

22.1. Os equipamentos *as a service* terão garantia e licenciamento pelo fabricante, conforme mencionado na Proposta Comercial da Contratada, contados do recebimento dos produtos pelo gestor/fiscalizador do contrato.

22.2. Durante o período de vigência do instrumento contratual a Contratada deverá substituir os equipamentos que apresentarem problemas de fabricação ou que denotem não serem novos ou ter sinais de uso anterior.

22.3. A garantia não cobre os danos causados pelo não atendimento das especificações operacionais, negligência ou mau uso dos equipamentos.

22.4. A garantia é intransferível e só beneficia a própria Universidade USCS, como adquirente original dos equipamentos, não compreende a reposição de partes e peças perecíveis e sujeitas ao desgaste natural.

22.5. Estão previstos, nessa garantia, os equipamentos adquiridos, sendo que quando apresentarem problemas, deverão ser consertadas ou substituídas no prazo de 5(cinco) dias úteis, com as mesmas características, sem nenhum ônus para a Universidade Municipal de São C. do Sul.

23. DAS DISPOSIÇÕES GERAIS

23.1. O presente Edital, seus anexos e a proposta da licitante vencedora integrarão o termo de contrato, independentemente de transcrição.

23.2. Da sessão pública para recebimento, julgamento de proposta de preços, e habilitação documental deste processo licitatório, lavrar-se-á ata circunstanciada, na qual serão registradas as ocorrências relevantes, inclusive os diálogos enunciados por meio da ferramenta do sistema de pregão eletrônico"chat".

23.3. É facultada ao pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar ou ter sido providenciado no ato da sessão pública.

23.4. O agente público pregoeiro e a equipe de apoio, se entenderem conveniente ou necessário, poderão se utilizar de assessoramento técnico e jurídico específicos para tomar decisões relativas ao presente certame licitatório, por meio de documento devidamente formalizado o qual integrará o respectivo processo.

23.5. A proponente que no prazo de validade da proposta de preços não venha a mantê-la, ou convocada para assinar o contrato concernente ao **lote 01 e/ou 02**, caso não o faça no prazo estipulado neste edital, perderá a garantia de proposta em favor da Universidade Municipal de São Caetano do Sul, sem prejuízo das demais sanções legais aplicáveis.

23.6. A devolução da garantia de proposta enunciada no item acima, quando prestada nas modalidades previstas nos incisos I e IV do parágrafo primeiro do artigo 96, dar-se-á após a homologação do certame e consequente contratação do objeto.

23.7. A autoridade superior poderá revogar a licitação por razões de interesse público, derivado de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo invalidá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado, sem que caiba direito a qualquer indenização.

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

23.9. Os proponentes assumem todos os custos de preparação e apresentação de sua proposta e a USCS não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

23.10. Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

23.11. O proponente que vier a ser contratado, ficará obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

23.12. Não havendo expediente na USCS ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no horário e local aqui estabelecido, desde que não haja comunicação do Pregoeiro em contrário.

23.13. Na contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na USCS.

23.14. O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta, durante a realização da sessão pública de pregão.

23.15. As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança do futuro contrato.

23.16. Qualquer pedido de **esclarecimento** em relação a eventuais dúvidas na interpretação deste instrumento convocatório e seus anexos, bem como de cópias da legislação mencionada, devem ser solicitados por meio de documento digitalizado e assinado, inseridos em campo próprio do Portal de Compras da Universidade Municipal de São Caetano do Sul através do link https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/ , ou enviado para o e-mail: licitacao@online.uscs.edu.br , ou ainda, podem ser solicitadas por escrito, ao pregoeiro, na Rua Maceió, 177, Bairro Barcelona, São Caetano do Sul/SP – CEP 09551-030, até três dias úteis antes da data marcada para a data de abertura do certame.

23.16.1. A íntegra da resposta aos esclarecimentos elaborados a partir dos questionamentos será divulgada no sítio eletrônico oficial da Universidade no link https://licitacao.uscs.edu.br/ e no portal de compras, via link https://pregaoeletronico.saocaetanodosul.sp.gov.br/uscs/, no prazo de até três dias úteis, limitado ao último dia útil anterior à data de abertura do certame.

23.17. A participação na presente licitação implica em ciência quanto à obrigação de assinar, juntamente com Contrato o "Termo de Ciência e Notificação" (de acordo com o anexo LC-01, da instrução do TCESP 001/2020), e que o descumprimento poderá gerar penalizações

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

23.19. Para as demais condições de contratação, observar as disposições constantes do Anexo I - Termo de Referência deste Edital.

23.20. Prazo para retirada do contrato ou instrumento equivalente de 05 (cinco) dias úteis.

23.21. Aos casos omissos aplicar-se-ão as demais disposições constantes da Lei Federal número 14.133/2021.

23.22. Para dirimir as questões oriundas deste Edital, não resolvidas na esfera administrativa, é competente o Foro da Comarca de São Caetano do Sul, por mais privilegiado que outro seja.

23.23. Integram o instrumento convocatório, conforme o caso:

ANEXO I TERMO DE REFERÊNCIA.

ANEXO II PROPOSTA COMERCIAL.

ANEXO III REDUÇÃO DE LANCES.

ANEXO IV DECLARAÇÃO DE REGULARIDADE PERANTE O MINISTÉRIO DO TRABALHO.

ANEXO V DECLARAÇÃO DE CUMPRIMENTO DAS CONDIÇÕES DE HABILITAÇÃO.

ANEXO VI DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA FRUIÇÃO DOS BENEFÍCIOS DA LEI COMPLEMENTAR Nº 123/2006 COM AS DEVIDAS ALTERAÇÕES INTRODUZIDAS PELAS LEIS COMPLEMENTARES FEDERAIS NÚMERS 147/2014 E 155/2016, E LEI MUNICIPAL Nº 4.660/2008.

ANEXO VII DECLARAÇÃO DE ATENDIMENTO ÀS NORMAS RELATIVAS À SAÚDE E SEGURANÇA NO TRABALHO.

ANEXO VIII DECLARAÇÃO DE CONDIÇÕES GERAIS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS.

ANEXO IX DECLARAÇÃO DE QUE A PROPOSTA ECONÔMICA CONTEMPLA TODOS OS CUSTOS TRABALHISTAS.

ANEXO X DECLARAÇÃO DE CUMPRE OS REQUISITOS DE RESERVA DE CARGOS PARA PESSOAS PORTADORAS DE DEFICIÊNCIA E REABILITADOS DA PREVIDÊNCIA SOCIAL.

ANEXO XI DECLARAÇÃO DE QUALIFICAÇÃO TÉCNICA DO PROFISSIONAL QUE SERÁ ALOCADO NO PROJETO.

ANEXO XII DECLARAÇÃO DE CREDENCIADO JUNTO AO FABRICANTE DO EQUIPAMENTO.

ANEXO XIII MINUTA DE CONTRATO E TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE DE PROTEÇÃO DE DADOS PESSOAIS.

ANEXO XIV TERMO DE CIÊNCIA E NOTIFICAÇÃO E DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TRIBUNAL DE CONTAS DO ESTADO - LC-01; LC-02 e PC 02.

ANEXO XV ESTUDO TÉCNICO PRELIMINAR

ANEXO XVI PLANO DE GESTÃO DE RISCO.

São Caetano do Sul, 03 de dezembro de 2025.

_____

Prof. Ms. Orlando Antônio Bonfatti
Pró-Reitor Administrativo e Financeiro

ANEXO I

TERMO DE REFERÊNCIA
Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

OBJETIVO

O presente Termo de Referência tem como objetivo a contratação de empresa especializada para fornecimento de infraestrutura e serviços de hospedagem em nuvem, bem como solução de segurança perimetral (Next Generation Firewall) para atendimento ao ambiente de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul.

1. Especificações e Exigências Aplicadas ao Lote 01

a. Unidades da Universidade Municipal de São Caetano do Sul a serem atendidos nesse projeto desses serviços:

O quadro imediatamente abaixo, há o detalhamento das unidades da Universidade de São Caetano do Sul que deverão realizar a contratação dos respectivos serviços destacados neste termo de referência.

DIMENSIONAMENTO	Universidade Municipal de São Caetano do Sul					
	UNIDADE BARCELONA Endereço: Av. Goiás, 3400 - Barcelona, São Caetano do Sul - SP, CEP: 09550-051.	UNIDADE CENTRO Endereço: R. Santo Antônio, 50 - Centro, São Caetano do Sul - SP, CEP: 09521-160.	UNIDADE CENTRO 2 Endereço: Rua Samuel Klein, 83 2° Andar - Centro - São Caetano do Sul - CEP: 09510-125.	UNIDADE CONCEIÇÃO Endereço: Rua Conceição, 321 - Santo Antônio - São Caetano do Sul - 09530-060.	UNIDADE ITAPETININGA Endereço: Av. Dr. Ciro Albuquerque, 4750 - Taboãozinho, Itapetininga - SP, CEP: 18200-021.	UNIDADE MANOEL COELHO Endereço: Rua Manoel Coelho, 600 - 6º andar - Centro, São Caetano do Sul - SP, Cep: 09510-101.
	Serviço tipo: 1.	**Serviço tipo: 1.**	**Serviço tipo: 3.**	**Serviço tipo: 2.**	**Serviço tipo: 3.**	**Serviço tipo: 3.**
	As unidades destacadas são as responsáveis por receber as instalações locais, garantindo que todo o processo de implementação e configuração seja realizado de forma adequada e eficiente. Essas unidades desempenham um papel fundamental na adaptação das soluções aos requisitos específicos de cada local, assegurando que os recursos necessários para o bom funcionamento das operações estejam corretamente instalados e configurados.					

b. No escopo dessa contratação, em particular o lote 01, essa administração tem a pretensão de contratar no mercado empresa com expertise para fornecer serviço de segurança de rede baseada em equipamento de firewall *as a service*, integrada a prestação de serviços de suporte técnico, manutenção e monitoramento no formato 24x7, por período de 24 meses. No quadro abaixo, relaciona-se os diversos serviços objeto de contratação e sua categorização.

A Contratada será responsável pela aquisição, entrega, implementação e configuração e licenciamento de todos os equipamentos *as a service* necessários e descritos no quadro a seguir desse documento, não sendo aceito a entrega de outros hardwares que não contemplem plenamente as especificações elencadas neste termo de referência.

	Item	Descrição	Quantidade em meses
LOTE 01		SERVIÇO DE SEGURANÇA FIREWALL *AS A SERVICE* TIPO **1**.	24
		SERVIÇO DE SEGURANÇA FIREWALL *AS A SERVICE* TIPO **2**.	24
		SERVIÇO DE SEGURANÇA FIREWALL *AS A SERVICE* TIPO **3**.	24
		SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	01
		SERVIÇO DE SUPORTE TÉCNICO COM ATENDIMENTO LOCAL E REMOTO	24
		SERVIÇO DE MONITORAMENTO (NOC)	24

1.1. SOLUÇÃO DE FIREWALL DE PROXIMA GERAÇÃO.

1.1.1. Deverá ser fornecida uma solução de firewall de próxima geração (NGFW – Next Generation Firewall) em alta disponibilidade, no modo ativo/ativo, ou seja, no mínimo dois equipamentos funcionando simultaneamente para todas as unidades da universidade.

1.1.2. Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos e efetuar os necessários ajustes sem ônus para o contratante desde que os danos causados não sejam decorrentes do mau uso, imperícia ou imprudência;

1.1.3. Os equipamentos devem ser iguais e suportar no mínimo as seguintes configurações e ser configuradas de acordo com ambiente:
1.1.4. Especificações Gerais:
1.1.4.1. Os equipamentos a serem utilizados deverá fornecer logs e relatórios embarcados, com armazenamento histórico mínimo de 120 dias, contendo no mínimo os itens abaixo:

- Dashboard com informações do sistema:
- Informações de CPU
- Informações do uso da rede.
- Informações de memória.
- Informações de atividades de navegação.
- Permitir visualizar número políticas ativas.
- Visualizar número de usuários conectados remotamente.
- Visualizar número de usuários conectados localmente.

1.1.5. Relatórios com informações sobre as conexões de origem e destino por países.
1.1.6. Relatórios informando as conexões dos hosts.
1.1.7. Visualizar relatórios por período, permitindo o agendamento e envio destes relatórios por e-mail.
1.1.8. Permitir exportar relatórios para as seguintes extensões/plataformas:

- PDF
- HTML
- Excel
- Permitir visualizar relatório de políticas ativas associado ao ID da política criada.
- Relatório que informe o uso IPSEC por host e usuário.
- Relatório que informe o uso L2TP por host e usuário.
- Relatório que informe o uso PPTP por usuários.
- Relatório abordando eventos de VPN.
- Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações:
- Logs do sistema;
- Logs das políticas de segurança;
- Logs de autenticação;
- Logs de administração do firewall NGFW.
- Permitir ocultar os relatórios usuários e IPs cadastrados.

➢ **TIPIFICAÇÃO DA SOLUÇÃO DE FIREWALL QUE SERÁ CONTRATADA**

1.1.9. **A SOLUÇÃO DO TIPO 1** deverá possuir no mínimo as seguintes configurações tanto quanto de software como de hardware:
1.1.9.1. Modalidade de configuração, alta disponibilidade e dois equipamentos configurados como ativo/ativo.
1.1.9.2. Possuir no mínimo 4 interfaces 10/100/1000 base-T;
1.1.9.3. Possuir no mínimo 4 interfaces 2,5GbE base-T;
1.1.9.4. Possuir no mínimo 4 interfaces SFP+ 10GbE;
1.1.9.5. Deve possuir no mínimo 2 portas que suportem by-pass;
1.1.9.6. Deve possuir no mínimo 2 portas que suportem by-pass;
1.1.9.7. A solução proposta deve corresponder aos seguintes critérios:

- Suportar no mínimo 368.000 novas conexões por segundo;
- Suportar no mínimo 16.600.000 conexões simultâneas;
- Possuir no mínimo 75 Gbps de rendimento (throughput) do Firewall;
- No mínimo 29.500 Mbps de rendimento (throughput) de IPS;
- Possuir no mínimo 3,2 (três inteiros e dois décimos) Gbps de throughput de VPN AES.
- Deverá possuir no mínimo 25.200 Mbps de taxa de transferência de Threat Protection.
- Latência do Firewall máxima (UDP de 64 bytes) 3 µs.
- IPsec VPN throughput deverá suportar no mínimo 62.500 Mbps.
- Quantidade mínima de túneis simultâneos VPN IPsec 8.500.
- Quantidade mínima de Túneis simultâneos SSL VPN 7.500.
- Inspeção SSL/TLS de 8.000 Mbps no mínimo.
- Deve possuir um interruptor de alimentação.
- Conexões SSL/ TLS simultâneas 276480.

1.1.10. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.1.11. A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
1.1.12. A solução proposta deve possuir no mínimo 240 GB de espaço em disco SSD SATA-III para o armazenamento local de eventos e relatórios.
1.1.13. Possuir pelo menos, 2 (dois) slots para adição de módulo de portas;
1.1.14. Deverá possuir Pinos de montagem para externo fonte de energia.
1.1.15. Ter o peso máximo após desembalado de 9 kg.
1.1.16. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
1.1.17. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
1.1.18. Deverá ter disponível pelo menos 2 conexões USB 3.0.
1.1.19. Não deverá possuir limitação na quantidade de VPN via Software.
1.1.20. Deverá possuir um display LCD, multifuncional e na parte frontal do firewall
1.1.21. Número irrestrito de usuários/IP conectados.
1.1.22. O equipamento deve ter no máximo 1 (um) U de altura para montagem em rack.

1.1.23. **A SOLUÇÃO DO TIPO 2** deverá possuir no mínimo as seguintes configurações tanto quanto de software como de hardware:
1.1.24. Modalidade de configuração, alta disponibilidade e dois equipamentos configurados como ativo/ativo.
1.1.25. Possuir no mínimo 8 interfaces 10/100/1000 base-T e 2 SFP 1GbE;
1.1.26. Possuir no mínimo 2 interfaces SFP+ 10GbE;
1.1.27. Deve possuir no mínimo 1 porta que suportem by-pass;
1.1.28. A solução proposta deve corresponder aos seguintes critérios:

- Suportar no mínimo 186.500 novas conexões por segundo;
- Suportar no mínimo 12.260.000 conexões simultâneas;
- Possuir no mínimo 47 Gbps de rendimento (throughput) do Firewall;
- No mínimo 10.500 Mbps de rendimento (throughput) de IPS;
- Deverá possuir no mínimo 7.400 Mbps de taxa de transferência do Threat Protection.
- Latência do Firewall máxima (UDP de 64 bytes) 4 µs.
- IPsec VPN throughput deverá suportar no mínimo 25.000 Mbps.
- Quantidade mínima de túneis simultâneos VPN IPsec 6.500.
- Quantidade mínima de Túneis simultâneos SSL VPN 5.000.
- Inspeção SSL/TLS de 2.470 Mbps no mínimo.
- Quantidade mínima de conexões simultâneas SSL/TLS de 55.290.
- Deve possuir um interruptor de alimentação.

1.1.29. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.1.30. A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
1.1.31. A solução proposta deve possuir no mínimo 240 GB de espaço em disco SSD SATA-III para o armazenamento local de eventos e relatórios.
1.1.32. Possuir slot para adição de módulo de portas;
1.1.33. Deverá possuir Pinos de montagem para externo fonte de energia.
1.1.34. Ter o peso máximo após desembalado de 5 kg.
1.1.35. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
1.1.36. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
1.1.37. Deverá ter disponível pelo menos 2 conexões USB 3.0 e 1 conexão 2.0
1.1.38. Não deverá possuir limitação na quantidade de VPN via Software.
1.1.39. Deverá possuir um display LCD, multifuncional e na parte frontal do firewall
1.1.40. Número irrestrito de usuários/IP conectados.
1.1.41. O equipamento deve ter no máximo 1 (um) U de altura para montagem em rack 19”.

1.1.42. **A SOLUÇÃO DO TIPO 3** deverá possuir no mínimo as seguintes configurações tanto quanto de software como de hardware:
1.1.43. Modalidade de configuração, alta disponibilidade e dois equipamentos configurados como ativo/ativo.
1.1.44. Possuir no mínimo 4 interfaces 10/100/1000 base-T;
1.1.45. Possuir no mínimo 2 interfaces 2,5 GbE base-T PoE de no mínimo 30w;
1.1.46. Possuir no mínimo 2 interfaces SFP+ 10GE fiber;
1.1.47. A solução proposta deve corresponder aos seguintes critérios:
- Suportar no mínimo 105.000 novas conexões por segundo;
- Suportar no mínimo 6.400.000 conexões simultâneas;
- Possuir no mínimo 19,1 Gbps de rendimento (throughput) do Firewall;
- No mínimo 5.800 Mbps de rendimento (throughput) de IPS;
- Deverá possuir no mínimo 4.750 Mbps de taxa de transferência do Threat Protection.
- IPsec VPN throughput deverá suportar no mínimo 6.350 Mbps.
- Quantidade mínima de túneis simultâneos VPN IPsec 2.500.
- Quantidade mínima de Túneis simultâneos SSL VPN 1.500.
- Inspeção SSL/TLS de 1.700 Mbps no mínimo.
- Quantidade mínima de conexões simultâneas SSL/TLS de 18.432.
- Deve possuir um interruptor de alimentação.

1.1.48. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.1.49. A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
1.1.50. A solução proposta deve possuir no mínimo 64 GB de espaço para o armazenamento local de eventos e relatórios.
1.1.51. Possuir slot para adição de módulo de portas;
1.1.52. Ter o peso máximo após desembalado de 3 kg.
1.1.53. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
1.1.54. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
1.1.55. Deverá ter disponível pelo menos 1 conexão USB 3.0 e 1 conexão 2.0
1.1.56. Não deverá possuir limitação na quantidade de VPN via Software.
1.1.57. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e console.
1.1.58. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup) das configurações, incluindo os objetos de usuário.
1.1.59. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.
1.1.60. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.
1.1.61. A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário.
1.1.62. A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory.
1.1.63. Suporte à autenticação do Chromebook.
1.1.64. Os tipos de autenticação devem ser, modo transparente, por autenticação NTLM e cliente de autenticação nas máquinas.
1.1.65. Fornecer clientes de autenticação para Windows, MacOS X, Linux 32/64.
1.1.66. Certificados de autenticação para iOS e Android.
1.1.67. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.
1.1.68. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.
1.1.69. A solução proposta deve suportar NTP.
1.1.70. A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.
1.1.71. A solução proposta deve ter suporte multilíngue para console de administração web.

1.1.72. A solução proposta deverá suportar fazer um rollback de versão.
1.1.73. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.
1.1.74. A solução proposta deve suportar instalação de LAN by-pass no caso do firewall NGFW estar configurado no modo transparente.
1.1.75. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que o PPPoE mudar.
1.1.76. A solução proposta deve suportar SNMP v1, v2c.
1.1.77. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.
1.1.78. A solução proposta deve ser baseada em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança.
1.1.79. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.
1.1.80. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação).
1.1.81. A solução proposta deve atender terminais (Microsoft) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.
1.1.82. A solução proposta deve suportar:
1.1.83. Serviço de DHCP/DHCPv6;
1.1.84. Serviço de DHCP/DHCPv6 Relay Agent;
1.1.85. A solução proposta deve trabalhar como DNS/DNSv6 Proxy.
1.1.86. Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting.
1.1.87. Permitir exportar informações de troubleshooting para arquivo PCAP.
1.1.88. Reutilização de definições de objetos de rede, hosts, serviços, período, usuários, grupos, clientes e servers.
1.1.89. Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades específicas a ele.
1.1.90. Controle de acesso e dispositivos por zoneamento.
1.1.91. Integrar com ferramenta de gerenciamento centralizado disponibilizado pelo próprio fabricante.
1.1.92. Traps SNMP ou e-mail para notificações do sistema.
1.1.93. Suportar envio de informações via Netflow e possuir informações via SNMP;

1.2. BALANCEAMENTO DE CARGA E REDUNDÂNCIA PARA MÚLTIPLOS PROVEDORES DE INTERNET

1.2.1. A solução proposta deve suportar o balanceamento de carga e redundância (Failover) para no mínimo 2 (dois) links de Internet.
1.2.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.
1.2.3. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga.
1.2.4. A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP.
1.2.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.
1.2.6. A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin".
1.2.7. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet, bem como tráfego IPv4 e IPv6.

1.3. ALTA DISPONIBILIDADE

1.3.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) no modelo ativo/ativo.
1.3.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways, mantendo a Alta Disponibilidade.
1.3.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.
1.3.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.
1.3.5. A solução proposta deve suportar sincronização automática e manual entre os firewalls NGFWs em "cluster".

1.3.6. A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge).

1.4. ESPECIFICAÇÕES DO FIREWALL E ROTEAMENTO

1.4.1. A solução deve ser Standalone Firewall NGFW e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança.
1.4.2. A solução proposta deve suportar “Stateful Inspection” baseado no usuário "one-to-one", NAT Dinâmico e PAT.
1.4.3. A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall.
1.4.4. A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga, baseado na mesma regra do Firewall para facilitar de uso.
1.4.5. A solução proposta deve suportar arquitetura de segurança baseado em Zonas.
1.4.6. A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".
1.4.7. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.
1.4.8. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).
1.4.9. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.
1.4.10. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.
1.4.11. O sistema proposto deve prover mensagem de alertas no Dashboard (Painel de Bordo) quando eventos como, por exemplo: nova firmware disponível para download ou a licença irá expirar em breve.
1.4.12. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address).
1.4.13. A solução proposta deve suportar IPv6.
1.4.14. A solução proposta deve suportar implementações de IPv6 Dual Stack.
1.4.15. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd.
1.4.16. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.
1.4.17. A solução proposta deve suportar DNSv6.
1.4.18. A solução proposta deve oferecer proteção DoS contra ataques IPv6.
1.4.19. A solução proposta deve oferecer prevenção contra Spoof em IPv6.
1.4.20. A solução proposta deve suportar 802.3ad para Link Aggregation.
1.4.21. A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga.
1.4.22. A solução proposta deve suportar gerenciamento de banda baseado em aplicação, que permite administradores criarem políticas de banda de utilização de link baseado por aplicação.
1.4.23. Flood protection, DoS, DDoS e Portscan.
1.4.24. Bloqueio de Países baseados em GeoIP.
1.4.25. Suporte a Upstream proxy.
1.4.26. Suporte a VLAN DHCP e tagging.
1.4.27. Suporte a Multiple bridge.
1.4.28. Funcionalidades do portal do usuário.
1.4.29. Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).
1.4.30. Download dos clientes de autenticação disponibilizados pela ferramenta.
1.4.31. Download do cliente VPN SSL em plataformas Windows.
1.4.32. Download das configurações SSL em outras plataformas.
1.4.33. Informações de hotspot.
1.4.34. Autonomia de troca de senha do usuário.
1.4.35. Visualização do uso de internet do usuário conectado.
1.4.36. Acesso a mensagens em quarentena.
1.4.37. Opções base de VPN.
1.4.38. Site-to-site VPN: SSL, IPSec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key.
1.4.39. L2TP e PPTP.

1.4.40. VPN SSL, IPSEC.
1.4.41. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

1.5. FUNCIONALIDADES BASE DE QOS E QUOTAS

1.5.1. QoS aplicado a redes e usuários de download/upload em tráfegos baseados em serviços.
1.5.2. Otimização em tempo real do protocolo VoIP.
1.5.3. Suporte a marcação DSCP.
1.5.4. Regras associadas por usuário.
1.5.5. Criar regras que limitem e garantam upload e download.
1.5.6. Permitir criar regra de QoS individualmente e compartilhada.

1.6. FILTRAGEM E SEGURANÇA WEB

1.6.1. Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web.
1.6.2. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas, agregadas a pelo menos 75 categorias oferecidas pela solução.
1.6.3. Realizar autenticação dos usuários nos modos transparente e padrão.
1.6.4. As autenticações devem ser feitas via NTLM.
1.6.5. Possuir sistema de quotas aplicado por usuários e grupos.
1.6.6. Permitir criar políticas por horário aplicado a usuários e grupos.
1.6.7. Possuir sistema de malware scanning que realize as seguintes ações:
- Bloquear toda forma de vírus
- Bloquear malwares web
- Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acesso web (via navegador).

1.6.8. Prover proteção em tempo real de todos os acessos web.
1.6.9. A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças.
1.6.10. Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.
1.6.11. Fornecer Pharming Protection.
1.6.12. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.
1.6.13. Permitir criação de regras customizadas baseadas em usuário e hosts.
1.6.14. Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy.
1.6.15. Validação de certificado.
1.6.16. Prover cache de navegação, contribuindo na agilidade dos acessos à internet.
1.6.17. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)
1.6.18. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.
1.6.19. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.
1.6.20. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.
1.6.21. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.
1.6.22. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.
1.6.23. Range aceitável de 1 a 25600KB.
1.6.24. Bloquear tráfego que não segue os padrões do protocolo HTTP.
1.6.25. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.
1.6.26. Nas exceções, permitir definir operadores “AND” e “OR”.
1.6.27. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.
1.6.28. Permitir definir nas exceções a opção de não realizar escaneamento contra malware.
1.6.29. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.

1.6.30. Permitir criar regras de exceções por endereços IPs de origem.
1.6.31. Permitir criar regras de exceções por endereços IPs de destino.
1.6.32. Permitir criar exceções por grupo de usuários.
1.6.33. Permitir criar exceções por categorias de sites.
1.6.34. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.
1.6.35. Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: “Criminal Activities, Finance & Investing, Games and Gambling”, entre outras.
1.6.36. Permitir editar grupos de categorias pré-estabelecidos pela solução.
1.6.37. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações:
- Nome da regra;
- Permitir criar uma descrição para identificação da regra.
- Ter a possibilidade de classificação de pelo menos: Produtivo ou Não produtivo;
- Permitir aplicar Traffic shaping diretamente na categoria.
- Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave.
- Deve permitir importar uma base com domínios e palavras-chaves na hora da criação da categoria, a base com informações de domínios e palavras-chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt.
- Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro.

1.6.38. Ter função para criar grupos de URLs.
1.6.39. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.
1.6.40. Permitir ao administrador especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.
1.6.41. Deve permitir que em uma mesma política sejam aplicadas ações diferentes de acordo com o usuário autenticado.
1.6.42. Nas configurações das políticas deve-se existir pelo menos as opções de: Liberar categoria/URL, bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.
1.6.43. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.
1.6.44. Permitir criar cotas de navegação com os seguintes requisitos:
1.6.45. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.

1.7. CONTROLE E SEGURANÇA DE APLICAÇÕES

1.7.1. Prover controle para mais de 2500 aplicações diferentes.
1.7.2. Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.
1.7.3. Permitir criar regras de controle por usuário e hosts.
1.7.4. Permitir realizar traffic shaping por aplicação e grupo de aplicações.
1.7.5. Possibilitar que as regras criadas baseadas em aplicação permitam:
- Bloquear o tráfego para as aplicações
- Liberar o tráfego para as aplicações
- Criar categorização das aplicações por risco:
- Risco muito baixo
- Risco baixo
- Risco médio
- Risco alto
- Risco muito alto

1.7.6. Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.

1.7.7. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.
1.7.8. Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao youtube, mas bloquear o upload de vídeos, e etc.
1.7.9. Permitir agendar um horário e data específica para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

1.8. PROTEÇÃO DE REDE

1.8.1. Prover funcionalidade de Intrusion Prevention System (IPS).
1.8.2. Proporcionar alta performance na inspeção dos pacotes.
1.8.3. Possuir mais de 6500 assinaturas conhecidas.
1.8.4. Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.
1.8.5. Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.
1.8.6. Possuir funcionalidade Anti-DoS.
1.8.7. Deve-se permitir customizar os valores das seguintes funcionalidades de DoS:
- SYN Flood
- UDP Flood
- TCP Flood
- ICMP Flood
- IP Flood

1.8.8. Possuir templates pré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ e etc.
1.8.9. Possuir proteção contra spoofing.
1.8.10. Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.
1.8.11. Possuir funcionalidade para o administrador poder criar by-pass de DoS.
1.8.12. Permitir ao administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.

1.9. PROTEÇÃO AVANÇADA CONTRA AMEAÇAS PERSISTENTES (APT)

1.9.1. Detectar e bloquear tráfego de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.
1.9.2. Possuir logs e relatórios que informem todos os eventos de APT.
1.9.3. Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.
1.9.4. Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.
1.9.5. Proteção para E-mails
1.9.6. Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.
1.9.7. Possuir serviço de reputação para monitoramento dos fluxos dos e-mails, sendo assim, o AntiSpam deverá bloquear e-mails considerados com má reputação na internet e pelo fabricante.
1.9.8. Bloquear SPAN e MALWARES durante a transação SMTP.
1.9.9. Possuir duas engines de antivírus para duplo escaneamento.
1.9.10. Ter proteção em tempo real, sendo que a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos e-mails que passam pela solução e assim tomar ações automáticas de segurança, caso necessário.
1.9.11. Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.
1.9.12. Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.
1.9.13. Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customizá-los de acordo com o desejado.

1.9.14. Ter suporte a criptografia TLS para SMTP, POP e IMAP.
1.9.15. As ações dos e-mails considerados SPAM devem ser:
- Drop
- Warn
- Quarantine

1.9.16. Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: SPAM Marketing etc. etc. etc.
1.9.17. Permitir visualizar os e-mails que se encontram na fila para serem enviadas.
1.9.18. Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.
1.9.19. Possuir funcionalidade de allowlist e blocklist.
1.9.20. Possuir funcionalidade que rejeite e-mails com HELO inválido e/ou que não possuam RDNS.
1.9.21. Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.
1.9.22. Prover ambiente de Sandbox na nuvem provido pelo próprio fabricante.
1.9.23. Realizar inspeções de executáveis e documentos que possuam conteúdo executáveis.
1.9.24. Possuir suporte aos principais executáveis Windows como: .exe, .com e .dll
1.9.25. Possuir suporte aos principais documentos do Word como: .doc, .docx, .docm e .rft.
1.9.26. Realizar análise em documentos PDF.
1.9.27. Realizar análise de qualquer tipo de conteúdo que possua os seguintes tipos de arquivos: ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet.
1.9.28. Suporte a mais de 20 tipos de arquivos e extensões.
1.9.29. Realizar análises dinâmicas de malwares e ameaças, rodando estes arquivos em ambientes reais e em produção, todos providos na nuvem pelo fabricante.
1.9.30. Relatórios detalhados das ameaças bem como visibilidade dos alertas na dashboard da solução.
1.9.31. O tempo em média das análises devem ser menores do que 120 segundos.
1.9.32. Suportar a análise de links de download em tempo real.
1.9.33. Permitir escolher pelo menos duas regiões para as quais os arquivos para análise devem ser enviados.
1.9.34. Possuir uma opção que permita a solução identificar automaticamente o caminho com menor latência para envio dos arquivos para análise.
1.9.35. Permitir o administrador criar exceções para aqueles eventos que serão considerados falsos positivos.
1.9.36. O firewall NGFW deve oferecer relatórios locais referente a todos os eventos registrados pela funcionalidade de Sandbox.
1.9.37. A solução deverá prover uma ferramenta distribuída pelo mesmo fabricante para gerenciamento centralizado de ambos os firewalls NGFWs adquiridos pela contratante.
1.9.38. A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar políticas de gerenciamento para um ou mais equipamentos e aplicá-los todos de uma única vez.
1.9.39. As políticas de configurações devem ter no mínimo as seguintes opções:
- Proteção e políticas de acesso web
- Controle de aplicativos
- IPS
- VPN
- E-mail
- Firewall

1.9.40. A solução deverá oferecer funcionalidade que permita o administrador criar templates de configuração, para que o administrador possa aproveitar as mesmas regras para novos firewalls NGFWs.
1.9.41. Deverá haver na dashboard da solução, indicadores que permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.
1.9.42. Possuir múltiplas formas de customização de warning thresholds.
1.9.43. Possuir flexibilização na hora da criação de grupos de firewall NGFWs gerenciados, sendo possível diferenciá-los como por exemplo: Região, modelo ou outro parâmetro.
1.9.44. Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos, com diferentes funções.

1.9.45. Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realiza das caso necessário.

1.10. ANÁLISE E MONITORAMENTO POR INTELIGENCIA ARTIFICIAL

1.10.1. O serviço de firewall deverá ter disponível API's de comunicação para integração com inteligência artificial voltada a cibersegurança.
1.10.2. A inteligência artificial deverá atender todos os equipamentos de firewall e ter compatibilidade com a estrutura ATIVO/ATIVO de firewall.
1.10.3. A inteligência artificial deverá monitorar todas as ações e regras de firewall para levantamento dos dados referentes as configurações executadas medindo o seu nível de efetividade.
1.10.4. Integrar-se aos sistemas de logs do firewall para coletar, analisar e correlacionar eventos de segurança.
1.10.5. A criação de logs deverá ser em tempo real.
1.10.6. Atuar como uma plataforma centralizada para gerenciar várias instâncias de firewalls, oferecendo visibilidade de toda a infraestrutura de segurança.
1.10.7. Em resposta a eventos ou ameaças detectadas, a solução pode disparar ações automáticas no firewall, como bloqueio de IPs, isolamento de dispositivos, ou alterações nas regras de firewall para mitigar riscos.
1.10.8. Deverá ajudar a configurar e gerenciar as políticas de segurança no firewall, permitindo ajustes em tempo real de acordo com as necessidades da organização.
1.10.9. Através da integração com o firewall, a solução deverá oferecer um painel de monitoramento em tempo real, com relatórios detalhados sobre o tráfego de rede, ataques detectados e atividades suspeitas.
1.10.10. Deverá identificar vulnerabilidades de segurança em dispositivos na rede e sugerir ou aplicar correções baseadas nas configurações do firewall.
1.10.11. Quando integrada com a proteção de firewall deverá entregar uma abordagem de segurança mais robusta, correlacionando eventos e tomando medidas mais eficazes para a proteção da rede em tempo real.
1.10.12. Integração com as funcionalidades de prevenção de intrusões (IPS) e proteção contra malware, para uma resposta rápida a ameaças emergentes.

1.11. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

1.11.1. Deverão ser instalados e configurados os itens físicos e lógicos seguindo os padrões e melhores práticas recomendadas na norma NBR ISO/IEC 27002 e conforme critérios definidos pela contratante;
1.11.2. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;
1.11.3. Prestar todos os esclarecimentos que lhe forem solicitados, atendendo prontamente a quaisquer reclamações;
1.11.4. Fornecer toda mão de obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;
1.11.5. Instalação física de todos os equipamentos em Rack disponibilizado no local de instalação;
1.11.6. Os equipamentos devem ser configurados em alta disponibilidade, no modo ativo/ativo, dois equipamentos funcionando simultaneamente e em caso de falha o outro continue em operação;
1.11.7. Deverá migrar ou executar configurações similares às configurações atuais implementadas no firewall, atualmente em produção na contratante. A Contratada, além de apontar Marca e Modelo do Firewall, deverá apresentar o projeto de migração completo do Firewall atual para o novo Firewall. Não será aceito um programa automatizado de importação de Regras, especialmente para Firewall com arquitetura diferente da tecnologia atual.
1.11.8. O projeto deve levar em conta a diferença de arquiteturas e demonstrar a preservação das políticas através das camadas.
1.11.9. O equipamento deve estar com firmware e/ou software na versão mais recente e estável recomendada pelo fabricante da solução;
1.11.10. A empresa quando contratada deverá elaborar um plano de implantação junto a Universidade Municipal de São Caetano do Sul, contendo a descrição de atividades a serem desenvolvidas, relatórios e diagramas com dados relevantes para efeito decisório, responsáveis pelas

atividades, cronograma de implementação, compondo o documento denominado “Projeto Executivo” tendo a visibilidade completa do projeto e seus status evolutivos. O documento deve ser entregue para a Contratante antes do início da instalação, em até 10 dias úteis a partir do 1º dia útil subsequente a assinatura do contrato. O Gestor do contrato analisará o documento e dará o aceite em um prazo máximo de 02 dias úteis. Havendo necessidade de adequações a empresa terá um prazo máximo de 02 dias úteis para apresentar o projeto readequado, que será reavaliado pelo Gestor para aprovação, em um prazo máximo de 01 dia útil.

1.11.11. Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno nas melhores práticas de configuração do produto e fabricantes;

1.11.12. As senhas configuradas no ambiente durante a instalação deverão ter requisito mínimo de 08 (oito) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;

1.11.13. Os profissionais técnicos quando em serviço na Universidade Municipal de São Caetano do Sul deverão apresentar documento de identificação com foto e identificação da empresa com os seguintes:

- RG/CNH;
- Estar devidamente uniformizado para identificação da empresa Contratada.

1.11.14. A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente.

1.11.15. Deverá ser apresentado catálogo oficial, contendo as especificações técnicas dos produtos, bem como a camada de serviços ofertados para verificação técnica do responsável pela contratação.

1.12. MONITORAMENTO

1.12.1. O serviço de monitoramento deverá ser composto de tecnologia que seja totalmente apartada do ambiente computacional e de servidores da Contratante.

1.12.2. A Contratada deverá disponibilizar um switch de 8 portas ou superior, para configurar as conexões de rede necessárias para o monitoramento do ambiente sem a necessidade de utilizar os switches da Contratante.

1.12.3. O switch deverá conter no mínimo os seguintes recursos:

- Capacidade de comutação: 20 Gbps.
- Tabela de endereços MAC no mínimo de: 8.000 mil.
- Memória interna de no mínimo: 256 MB.
- Memória Flash mínima de 32 MB
- Buffer de pacote mínimo de 512 kb.
- Suportar até 256 VLANS simultaneamente e 4.000 mil Ids de VLAN.
- Interface das 8 portas em 10/100/1000 BASE-T ou superior.
- SFP de 1GB no mínimo de 2 Interfaces.
- Interruptor de liga e desliga com entrada DC-in
- Deverá ser 110w.

1.12.4. A Contratante não vai disponibilizar hardware ou software para que a Contratada realize o monitoramento.

1.12.5. Caso o hardware do monitoramento apresente alguma falha, a Contratada terá o prazo de até 1 hora para realizar a substituição nas unidades do Campus Barcelona, Centro, Centro 2, Conceição, e Lato Sensu (Manoel Coelho).

1.12.6. Caso o hardware do monitoramento apresente falha, a Contratada terá o prazo de até 5 horas para realizar a substituição na unidade Campus Itapetininga.

1.12.7. A Contratante não será responsável por armazenar hardware ou software para a substituição.

1.12.8. A fonte de carregamento e gerenciamento de energia deverá ser conectada através da porta tipo-C.

1.12.9. A Contratante não disponibilizará recursos computacionais para a instalação do sistema de monitoramento.

1.12.10. O recurso tecnológico poderá consumir até uma tomada do rack com o tipo padrão NBR 14136 de três pinos.

1.12.11. O recuso tecnológico deverá ser acompanhado com uma fonte de 100/240 VA, padrão NBR 14136 de três pinos, com botão que tenha a possibilidade de ligar e desligar o recurso

energético da fonte, deverá entregar 5V de 3000mA e o fio de conexão com a fonte de energia não deverá ser superior a 100cm.

1.12.12. Deverá possuir uma entrada do tipo RJ-45 com a velocidade de Gigabite 10/100/1000.
1.12.13. Deverá possuir 2 entradas USB 2.0.
1.12.14. Deverá possuir 2 entradas de USB 3.0.
1.12.15. Deverá possuir 2 entradas Micro HDMI 2.0.
1.12.16. O recurso tecnológico de monitoramento deverá ter suporte para sistema operacional Linux.
1.12.17. O recurso tecnológico deverá ser um dispositivo para que monitore toda a infraestrutura contratada neste termo de referência.
1.12.18. A comunicação com o datacenter deverá ser feita através do protocolo de comunicação TCP.
1.12.19. O recurso tecnológico deverá possuir um cooler para que ele consiga realizar a dissipação de calor assim evitando qualquer tipo de impacto no serviço de monitoramento.
1.12.20. O recurso tecnológico deverá possuir furação para que a dissipação de calor seja mais eficiente;
1.12.21. O recurso tecnológico deverá possuir o armazenamento em MicroSD de no mínimo 64gb;
1.12.22. A Contratada ficará responsável em realizar a entrega do recurso tecnológico juntamente com as respectivas licenças do sistema operacional e softwares de segurança como licença contra-ataques cibernéticos, backup do sistema operacional e até mesmo monitoramento do sistema tecnológico.
1.12.23. A solução deve ser concebida nativamente sobre uma arquitetura distribuída de múltiplos agentes de software autônomos, sendo no mínimo 6 agentes de IA, não podendo ser um mero agregado de ferramentas de terceiros.
1.12.24. Cada agente deve ser um processo de baixo impacto (low footprint) em termos de consumo de CPU e memória, capaz de operar de forma contínua no ativo (servidor, computador, etc.) sem degradar sua performance.
1.12.25. Os agentes de IA utilizaram o seu conhecimento para orquestrar atividade nos ativos, de acordo com a demanda as atividades serão auditadas, executadas e documentadas.
1.12.26. A IA e os seus agentes devem ser o motor de orquestração central, utilizando um modelo de Gráfico de Conhecimento (Knowledge Graph) para mapear dinamicamente e em tempo real os relacionamentos entre todos os ativos do ambiente (identidades, dispositivos, aplicações, dados, vulnerabilidades, etc.) e organizá-los em um contexto de dados no qual os agentes tenham a capacidade de personalizar a interação do usuário, diminuir a complexidade, aumentar a qualidade e a produtividade.
1.12.27. A plataforma deve ser capaz de, a partir da análise deste gráfico, inferir cadeias de ataque (Cyber Kill Chains) complexas e multivetoriais, correlacionando eventos de baixa relevância que, isoladamente, não seriam considerados ameaças.
1.12.28. A resposta a incidentes deve ser dinâmica e contextual, baseada nas inferências do motor cognitivo, superando a execução de fluxos de trabalho estáticos e lineares.
1.12.29. A solução de segurança com inteligência artificial para detecção e resposta estendida a incidentes na camada de proteção nos servidores, deverá ser totalmente compatível com a estrutura em cloud.
1.12.30. A contratação da prestação dos serviços e a disponibilização da ferramenta deverão atender integralmente aos normativos emitidos pelos órgãos fiscalizadores e de controle competentes, em especial ao disposto na Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).
1.12.31. A plataforma deve contar com agentes da Inteligência Artificial para auxiliar em toda a etapa da investigação.
1.12.32. A plataforma deve disponibilizar comunicação direta por texto com os agentes da Inteligência Artificial
1.12.33. A plataforma deve disponibilizar durante a navegação, interação com a Inteligência Artificial e acesso aos dados investigados.
1.12.34. A plataforma deve utilizar diferentes agentes da Inteligência Artificial para investigação de endpoints, alertas e Inteligência de ameaças.
1.12.35. A inteligência Artificial deve ser capaz de buscar todos os endpoints cadastrados, alertas abertos e vulnerabilidades identificadas na interação por texto e o resultado deve ser retornado em tela.

1.12.36. Os agentes de Inteligência devem ser capazes de correlacionar todos os dados coletados, analisar e fornecer um parecer investigativo sobre quais ações foram e/ou devem ser realizadas.
1.12.37. Deve usar um modelo matemático gerado a partir de aprendizado de máquina para comparar diferentes características de um arquivo executável, de forma estática, para determinar se ele é malicioso.
1.12.38. A plataforma deve ser capaz de detectar vazamentos de dados relacionados à Contratante, indicando o tipo de dado exposto e as datas que ocorreram.
1.12.39. A plataforma através dos agentes da Inteligência Artificial deve ser capaz de reclassificar a pontuação de risco da ameaça de acordo com a técnica explorada e a classificação do ativo;
1.12.40. A plataforma deve ser capaz de se integrar a aplicações e equipamentos da Contratante para enriquecer a detecção e resposta estendida em tempo real;
1.12.41. A proteção deve estar disponível para os sistemas operacionais Windows, Linux e MacOS.
1.12.42. Prevenção de ameaças baseada em comportamento para análise dinâmica de processos em execução.
1.12.43. Prevenção de exploração por técnicas conhecidas de exploits.
1.12.44. Prevenção de exploração baseada em kernel.
1.12.45. Prevenção de ameaças com base em inteligência de ameaças, como hash de arquivos.
1.12.46. Integração automatizada com um serviço de prevenção de malware, baseado em nuvem do próprio fabricante.
1.12.47. A solução deve prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros.
1.12.48. A solução deve ser compatível, no mínimo, com os seguintes sistemas operacionais e distribuição:
- Linux ou Windows.

1.12.49. A solução deve incluir na análise de execução, no mínimo, as seguintes características:
- Táticas e técnicas de acordo com o modelo de ameaças MITRE ATT&CK;
- Caraterísticas comportamentais suspeitas;
- Detalhes do arquivo como nome, hash, tamanho, tipo;
- Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
- Leitura e escrita de arquivos em disco;
- Leitura e alteração de chaves de registro.

1.12.50. Detalhes de processos iniciados durante a execução.
1.12.51. Atualizações transparentes do mecanismo de detecção de ameaças.
1.12.52. Proteção contra malware, ransomware e ataques sem arquivo.
1.12.53. Identificação e prevenção de tentativas de escalonamento de privilégios ao nível de Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux.
1.12.54. Deve permitir gerar alertas das soluções integradas.
1.12.55. Deve permitir a consulta de eventos de forma integrada.
1.12.56. Os usuários locais da solução devem ter uma política de senha que permita, no mínimo as seguintes configurações, alteração no primeiro login e identificação de complexidade de senha.
1.12.57. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless).
1.12.58. No caso de detecção de um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos.
1.12.59. A solução deve disponibilizar o rastreio de detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências.
1.12.60. A solução deve disponibilizar o rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante.
1.12.61. A solução deve disponibilizar o rastreio de tentativas de roubo de credenciais e\ou tentativa de acessos indevidos a recursos chave do sistema operacional.

1.12.62. Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa artefatos, destacando rapidamente índices de comprometimento já conhecidos.
1.12.63. Gerenciamento unificado e centralizado de todas as funções na mesma console de, bem como a instalação e atualização dos agentes.
1.12.64. Detecção de comprometimento: vírus, malware, backdoors, hosts em comunicação com sistemas infectados por botnet, serviços da Web vinculados a conteúdo malicioso.
1.12.65. Frequência de atualização, personalizável por dia, semana ou mês.
1.12.66. Varredura em tempo real de arquivos (gravação, renomeio e leitura) e de processos em memória.
1.12.67. Monitoramento em tempo real para captura de malwares que são executados em memória sem a necessidade de escrever em arquivo.
1.12.68. Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise comportamental, realizado por inteligência artificial.
1.12.69. Solução única para proteção contra malwares e ransomware, com a capacidade de coletar dados de sistemas operacionais e de rede para detecção de eventos maliciosos, sem a obrigatoriedade de criação e ativação de regras manualmente.
1.12.70. A solução deve permitir instalação silenciosa do agente, em sistemas operacionais Windows, através de pacotes MSI e executável EXE.
1.12.71. A solução deverá ser capaz também de analisar ameaças, sem o uso de assinaturas, fazendo esta análise por comportamento.
1.12.72. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações.
1.12.73. A solução deve suportar nativamente a integração com terceiros, sem a necessidade de instalação de recursos adicionais para receber eventos de múltiplas fontes de origem.
1.12.74. A solução deve disponibilizar, informações sobre o número de dispositivos que possuem o agente instalado e a versão do agente.
1.12.75. A solução deve ser capaz de monitorar o serviço de e-mail e domínio para identificar vazamento de dados.
1.12.76. Requisitos de detecção e resposta do agente
1.12.77. A solução não deve ter limitação para recebimento de eventos.
1.12.78. A comunicação entre agente e plataforma deve acontecer através do protocolo TCP porta 443;
1.12.79. O agente deve permitir a sua instalação em sistema operacional Linux Ubuntu 24.04 ou superiores.
1.12.80. A solução deve utilizar criptografia para conexão entre agente e plataforma, no mínimo, TLS 1.3 com AES 256.
1.12.81. A solução deve utilizar criptografia nos dados enviados para a plataforma de gerenciamento, no mínimo, AES 256.
1.12.82. A solução deve utilizar algoritmos de aprendizado de máquina para identificar padrões e comportamentos suspeitos.
1.12.83. A solução deverá ser capaz de bloquear tanto ameaças conhecidas como também as desconhecidas.
1.12.84. O agente deve detectar e proteger o dispositivo mesmo offline.
1.12.85. O agente deve receber atualizações de forma automática.
1.12.86. O agente deve receber as novas assinaturas de segurança em tempo real.
1.12.87. A solução deve utilizar detecção de ameaças por meio de dados e padrões baseados em comportamentos, que se utilizam de motores baseados em aprendizado de máquina para averiguação de arquivos.
1.12.88. O agente deve possuir a funcionalidade de inteligência contra malware.
1.12.89. O agente deve possuir a funcionalidade de inteligência contra ransomware.
1.12.90. O agente deve possuir a funcionalidade de bloqueio de indicadores de comprometimento.
1.12.91. O agente deve disponibilizar na sua interface, os seguintes dados:
1.12.91.1. Nome do usuário logado;
1.12.91.2. Nome do host;
1.12.91.3. Informações de sistema operacional (Build, Plataforma);
1.12.91.4. Estado do equipamento (Online ou Offline);

1.12.91.5. Última data comunicação com a console de gerenciamento;
1.12.91.6. Informações relacionadas à rede (IP, DNS, DHCP).
1.12.92. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela contratada.
1.12.93. A solução deve operar em tempo real, monitorando e bloqueando as ameaças.
1.12.94. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes.
1.12.95. A solução deve fornecer a capacidade de executar análises de estações de trabalho/servidores sem a necessidade de interagir com o usuário. Essa capacidade deve ser centralizada e transparente para o usuário.
1.12.96. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger e atualizar.
1.12.97. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho.
1.12.98. A solução deve ser capaz de fazer análise avançada e utilizar algoritmos de aprendizado de máquina, mesmo que sem conexão ao servidor de gerenciamento.
1.12.99. Consulta APIs: Capacidade de extrair dados de segurança e eventos para integração, utilizando os protocolos SSH, HTTP, SNMP e Syslog em todos os itens fornecidos dentro da solução proposta.
1.12.100. A solução deve disponibilizar um agente instalável e compatível com sistemas operacional, Windows, Linux e MacOS. Com a capacidade de detectar, coletar e enviar a plataforma, comportamentos maliciosos de aplicações que estão sendo executadas no sistema operacional.
1.12.101. A solução deve disponibilizar um coletor com capacidade de executar consultas de coleta de eventos e detecção de ação maliciosas em suas integrações, mesmo se houver indisponibilidade de conectividade.
1.12.102. Atualizações regulares e automáticas de binários e base de dados de segurança.
1.12.103. O agente deve ser compatível com o sistema operacional Linux Ubuntu 24.04 ou superiores.
1.12.104. A solução deve suportar a integração baseada em agente e autenticação.
1.12.105. A solução deve permitir o recebimento de eventos por múltiplos coletores.
1.12.106. A solução deve identificar os eventos por integração e agente.
1.12.107. A solução deve permitir a classificação de severidade, quando cadastrado o dispositivo.
1.12.108. Quanto ao armazenamento
1.12.108.1. A solução deve prover no mínimo 2TB de armazenamento para retenção dos eventos coletados e normalizados pela solução, sem custo adicional ou necessidade de fornecimento de hardware para armazenamento pela Contratante.
1.12.108.2. O evento armazenado pela solução, bem como hardware necessário para tal, é de responsabilidade da Contratada em armazenar em datacenter.
1.12.108.3. Solução deve ter a capacidade de permitir que a USCS modifique o período de armazenamento de eventos de Windows, Linux e Firewall de forma independente e através de plataforma gráfica disponibilizada pela solução proposta pela Contratada.
1.12.109. Quanto a Relatórios e Dashboards.
1.12.110. Visualização de Dados.
1.12.111. Painéis de controle para visualização em tempo real de incidentes e status de segurança.
1.12.112. Relatórios sobre incidentes, tendências de segurança e desempenho do sistema, exportando em formatos pdf, csv e html.
1.12.113. A solução deve ter capacidade de enviar relatórios através dos protocolos SMTP, HTTP, SFTP e ter integração com soluções de colaboração.

1.13. RELÁTORIOS

1.13.1. Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, com relatório de chamados referentes ao serviço descrito nesse lote:
1.13.2. Categoria do chamado;
1.13.3. Usuário;
1.13.4. Ativos relacionados;
1.13.5. Data de abertura e fechamento;

1.13.6. Status;
1.13.7. Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):
1.13.8. Disponibilidade;
1.13.9. Consumo de hardware (CPU, memória, disco, consumo de banda);
1.13.10. Alertas e erros.

1.14. SUPORTE TÉCNICO

1.14.1. Os serviços de suporte técnico especializado, deverão contemplar toda a solução e infraestrutura de segurança contidas neste Termo de Referência.

1.14.2. A USCS poderá abrir chamados de manutenção através de chamada telefônica para número com DDD (11), central de atendimento via navegador (WEB) ou correio eletrônico sem a necessidade prévia consulta e/ou qualquer liberação por parte da Contratada;
1.14.3. O atendimento técnico remoto deverá ocorrer 24 horas por dia.
1.14.4. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas de hardware e/ou software;
1.14.5. Toda falha e indisponibilidade no ambiente ocasionado por falhas físicas nos equipamentos (hardware) será de plena responsabilidade da Contratada.
1.14.6. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos;
1.14.7. Será de responsabilidade da Contratada manter o pleno funcionamento das políticas de segurança da solução.
1.14.8. Deverá monitorar diariamente, os relatórios de segurança gerados ao concluir as tarefas, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da Contratada efetuar correção ou ajuste técnico para a normalização dele, garantindo o pleno funcionamento da solução;
1.14.9. A Contratada deverá ser responsável por executar as restaurações do ambiente.
1.14.10. A empresa Contratada se responsabilizará pelas despesas com material de escritório, reprodução de documentos (cópias, etc.) e materiais diversos, que forem necessários à execução dos serviços de manutenção dos serviços e pelos seus profissionais;
1.14.11. A Contratada deverá realizar atendimentos remotos à equipe da Diretoria de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul, a partir de solicitações recebidas dos técnicos ou gestores do instrumento de contrato a ser celebrado com o vencedor do certame, via sistema de atendimento, telefone ou correio eletrônico;
1.14.12. Os atendimentos presenciais terão o prazo de até 1 hora para iniciar o atendimento nas unidades do Campus Barcelona, Centro, Centro 2, Conceição, e Lato Sensu (Manoel Coelho) e após a constatação técnica da Contratada.
1.14.13. O atendimento presencial terá o prazo de até 5 horas para iniciar o atendimento na unidade Campus Itapetininga após a constatação técnica da Contratada.
1.14.14. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados;
1.14.15. Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências;
1.14.16. Manter o ambiente de segurança sempre atualizado em com as melhores práticas aplicadas;
1.14.17. A Contratada deverá garantir que os profissionais designados para atendimento técnico serão capacitados;
1.14.18. A garantia de tempo de resposta será realizada conforme critérios de prioridades a seguir:

Classe	Descrição	Início do Atendimento em Até
1	Serviço indisponível	1 hora
2	Suporte técnico de maior impacto	4 horas
3	Suporte técnico com menor impacto	8 horas
4	Manutenção preventiva	Programada

1.14.19. O acordo de nível de serviço **(SLA)** para suporte técnico deverá obedecer ao seguinte escopo, respeitando-se as particularidades de cunho localização geográfica das Unidades.

PRIORIDADE	DESCRIÇÃO
1 (Emergencial)	O serviço está fora de operação ou há um impacto crítico nas operações.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações que sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

1.14.20. As horas para primeiro atendimento e resolução de incidentes são horas corridas e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

1.14.21. Caso seja identificado que o Serviço de Segurança se encontra indisponível por causa de soluções de terceiros, link de internet, indisponibilidade de switch, energia elétrica, roteadores, firewall, problemas de hardware/infraestrutura de TI ou qualquer serviço que interligue as unidades, será de responsabilidade da Contratada em realizar a detecção e resolução do problema.

1.14.22. A Contratada deverá disponibilizar e gerenciar os atendimentos técnicos da Universidade Municipal de São Caetano do Sul através de portal de gerenciamento de atendimentos com acesso através de navegador web;

1.14.23. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central;

1.14.24. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;

1.14.25. A Contratada deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento;

1.14.26. A USCS deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail;

1.14.27. O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da empresa Contratada, sendo essa responsável por sua atualização e manutenção;

1.14.28. A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;

1.14.29. O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;

1.14.30. A Contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela USCS;

1.14.31. Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;

1.14.32. Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a Universidade USCS;

1.14.33. O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a Contratante;

1.14.34. Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;

1.14.35. A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";

1.14.36. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;

1.14.37. Deverá ser possível a criação de grupos de usuários na solução;

1.14.38. A solução disponibilizada pela empresa Contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.
1.14.39. Relatórios Mensais, durante o período do contrato
1.14.40. Relatório de Chamados:
1.14.41. Categoria do chamado;
1.14.42. Usuário;
1.14.43. Ativos relacionados;
1.14.44. Data de abertura e fechamento;
1.14.45. Status;
1.14.46. O suporte técnico deverá ter os seguintes canais de atendimento: Suporte Telefônico, E-mail e Sistema online de chamados, todos em português do Brasil;
1.14.47. A empresa Contratada deverá sempre disponibilizar versões mais recentes dos softwares sem ônus financeiro para a Universidade;

1.15. MANUTENÇÃO PREVENTIVA DA SOLUÇÃO DE INTELIGENCIA ARTIFICIAL

1.15.1. A manutenção preventiva será destinada a atualizar os componentes de software (atualização tecnológica), conforme definições nesse documento, e a realizar quaisquer operações que evitem uma parada total ou parcial da solução.
1.15.2. A USCS, através de sua equipe técnica de Tecnologia da Informação, observará o desempenho do sistema contratado e, caso necessário, solicitará à Contratada a manutenção preventiva para viabilizar o melhor desempenho da solução.
1.15.3. A manutenção preventiva está inclusa no suporte técnico da solução, sendo prestada pela Contratada sem qualquer ônus adicional para a Contratante.
1.15.4. Durante a manutenção preventiva, a Contratada deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta.
1.15.5. Durante o período de suporte técnico deverá ser realizada a atualização de qualquer outro software constituinte da solução para as versões mais recentes, sem ônus adicional para a Universidade USCS.
1.15.6. A manutenção corretiva será destinada a remover erros ou falhas apresentadas pelos componentes de software da solução contratada.
1.15.7. Como erro ou falha entende-se a geração de resultado diferente do previsto. Para a resolução desses erros, é necessária a intervenção técnica especializada ou mesmo até a substituição de seus componentes por parte da empresa Contratada.
1.15.8. A manutenção corretiva após o diagnóstico (determinação da origem da falha) deverá ser realizada por meio de ajustes, consertos ou substituição dos elementos que apresentam problemas, restabelecendo a solução suas condições normais de funcionamento ou operação, conforme as especificações do fabricante.
1.15.9. Entende-se como diagnóstico à compilação e análise de informações para definição da causa de um problema.
1.15.10. Entende-se como Recuperação da Disponibilidade a execução de atividades que permitem restabelecer o funcionamento da solução.
1.15.11. A comprovação de isenção de responsabilidade se dará pela apresentação de relatório técnico circunstanciado dos elementos da solução contratada, e pelas demais informações consideradas necessárias pela Contratada para embasar a justificativa.
1.15.12. Tomar todas as providências necessárias para que seus funcionários, representantes e/ou contratados observem os regulamentos, normas e instruções de Segurança da Informação e Comunicações da USCS, quando estiverem executando serviços.
1.15.13. A Contratada deve comprometer-se a manter informações confidenciais no mais estrito sigilo sobre todos os dados, configurações, processos, fórmulas, rotinas e quaisquer outros objetos que sejam disponibilizados pela USCS à Contratada, para a realização dos trabalhos. Compromete-se a não copiar, não usar em seu próprio benefício, nem revelar ou mostrar a terceiros, nem divulgar tais informações, no território brasileiro ou no exterior, sob pena prevista em lei. Só os representantes e prepostos, devidamente autorizados entre as partes, cuja avaliação das informações confidenciais seja necessária e apropriada, para os propósitos especificados em contrato, terão acesso às mesmas.

1.15.14. Prestar os esclarecimentos necessários a Contratante, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.

1.15.15. Requisitos sociais, ambientais e culturais.

1.15.16. Sistema e todos os seus módulos devem ser desenvolvido/disponibilizado de forma compatível para as características do Brasil quanto a aspectos de interface gráfica, linguagem, legislação, costumes, apresentação, funcionalidades, telas e relatórios. Deve também possuir manuais de usuário online, com possibilidade de impressão, e documentação técnica do software em idioma português do Brasil ou inglês.

2. Especificações e Exigências Aplicadas ao Lote 02

Com relação ao **lote 02**, a Universidade Municipal de São Caetano do Sul pretende satisfazer a necessidade específica relacionada ao fornecimento de toda a infraestrutura em nuvem privada, necessária para equacionar a demanda de serviço de hospedagem em data center e hosting, gestão e monitoramento cloud computing de sua estrutura computacional, incluindo máquinas virtuais, link de acesso, segurança da informação, migração de suas aplicações e base de dados, bem como suporte técnico e monitoramento 24x7 da infraestrutura virtual a partir da contratação de empresa detentora desse *Know-how* por período de 24 meses.

Abaixo descreve-se a relação de serviços integrantes desse lote, bem como suas especificidades.

	Item	Descrição	Quantidade em meses
LOTE 02		SERVIÇO DE DATA CENTER HOSTING.	24
		SERVIÇO DE SUPORTE TÉCNICO.	24
		SERVIÇO DE MONITORAMENTO (NOC)	24
		SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	01

2.1. DATA CENTER HOSTING

2.1.1. A estrutura computacional em hosting deverá respeitar rigorosamente este termo de referência.

2.1.2. Os equipamentos ofertados devem ser novos, sem uso anterior.

2.1.3. O serviço de data center in cloud deverá possuir dois servidores totalmente compatíveis com alta disponibilidade.

2.1.4. Todo o licenciamento do ambiente em cloud deverá ser responsabilidade da Contratada.

2.1.5. Todo o licenciamento disponibilizado para esse projeto deverá ser da Microsoft.

2.1.6. Os dois servidores deverão ser iguais, do mesmo fabricante, sem modificações ou alteração do escopo de configuração.

2.1.7. Ambos os servidores deverão possuir compatibilidade com as configurações de tecnologia em alta disponibilidade.

2.1.8. As especificações do servidor tanto como o modelo do servidor, no ato da proposta comercial, deverão ser apresentadas para a validação computacional.

2.2. ESPECIFICAÇÕES DO PROCESSADOR

2.2.1. Cada servidor deverá ter no mínimo 2 (dois) processadores.

2.2.2. Cada processador deverá ter 16 Core.

2.2.3. Cada processador deverá ter 32 Threads.

2.2.4. Cada processador deverá ter no mínimo 3.0GHz.

2.2.5. Cada processador deverá ter no mínimo 64MB de cache.

2.2.6. O processador deverá estar em linha de produção fora do prazo de fim de vida/suporte técnico.

2.2.7. Deverá suportar virtualização.

2.3. ESPECIFICAÇÕES DA MEMORIA RAM:

2.3.1. Cada servidor deverá ter no mínimo 2 (dois) processadores.

2.3.2. Cada servidor ter 1TB de memória RAM disponível para a utilização.

2.3.3. A velocidade da memória RAM deverá ser DDR5 RDIMM 5600MHz.

2.4. ESPECIFICAÇÕES DO ARMAZENAMENTO:

2.4.1. Os servidores deverão atender os requisitos de armazenamento:

2.4.2. Deverá ter no mínimo o espaço de 400GB de disco SSD em RAID-1;

2.4.3. Deverá ter no mínimo o espaço em disco de 7TB com a taxa de escrita em até 10k em tecnologia SAS, em RAID-5;

2.4.4. Deverá ter no mínimo o espaço em disco de 6TB sendo a tecnologia SSD SATA em RAID-5.

2.5. COMUNICAÇÃO ENTRE OS SERVIDORES

2.5.1. Os servidores deverão se comunicar em 40GB.

2.5.2. A conectorização de comunicação obrigatoriamente deverá ser em QSFP.

2.6. CARACTERÍSTICAS FÍSICAS DO DATA CENTER

2.6.1. O Data Center in cloud deverá ser localizado no **Estado de São Paulo** para evitar alta lentidão.

2.6.2. Será de responsabilidade da Contratada implementar e configurar toda a estrutura contratada pela Universidade Municipal de São Caetano nesse termo de referência (lote 02).

2.6.3. O Data Center deverá atender no mínimo no que se refere as certificações Tier III ou ISO27001 ou SOC 2 Type 2;

2.6.4. O licenciamento e operação do ambiente em nuvem será de total responsabilidade da empresa vencedora do certame a ser contratada;

2.6.5. A Contratada deverá garantir a segurança da informação dos dados e estrutura em nuvem que irá hospedar os dados da USCS.

2.6.6. O Data Center deverá ter a estrutura de firewall, em alta disponibilidade e que supra a necessidade de transferência de dados.

2.6.7. O ambiente de firewall não poderá ter limite de conexões VPN.

2.6.8. Não será aceito nenhuma appliance de firewall genérica.

2.6.9. Não será aceito nenhuma appliance de firewall sem fabricante que possa desenvolver atualizações e vacinas.

2.6.10. O ambiente deverá ter a tecnologia de duplo fator de autenticação para acessar o ambiente computacional em cloud.

2.6.11. As instalações físicas do data center deverão ter os seguintes itens:

- Sistema de piso elevado, com vias independentes de cabos de energia, lógicos e óticos;
- Deverá possuir vias de energia elétrica e lógica em alta disponibilidade;
- Sistema de proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento.

2.6.12. A estrutura de energia elétrica do data center deverá atender aos seguintes requisitos:

- Alimentação elétrica redundante;
- Total independência no fornecimento de energia na eventualidade de falha na subestação que atende ao data center;
- Solução de grupo gerador redundante e independente (n+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia e com capacidade mínima de funcionamento por 72 horas com combustível local;
- Mínimo de 2KVAs nominais;
- Alimentação elétrica redundante e independente para os equipamentos da solução.

2.6.13. O Data Center que alocará o ambiente computacional da USCS e deverá atender os seguintes requisitos de climatização:

- Sistema de climatização com controles de temperatura, umidade relativa do ar e filtros de poeira;
- Sistema de climatização redundante (n+1), refrigerado por formas diferentes;
- Temperatura constante de 20ºC +/- 2ºC e umidade relativa do ar constante de 50% +/-10%.

2.6.14. O Data Center que alocará o ambiente computacional da USCS e deverá atender os seguintes requisitos de proteção contra incêndio:

- Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);
- Sistema automático de extinção de incêndios, baseado em agentes gasosos não poluentes, com ação baseada na quebra das moléculas de Oxigênio, do tipo FM200 e/ou FE227, ou equivalente, não nocivos aos equipamentos e seres humanos e que atenda a padrões internacionais;

- Sistema de detecção de incêndio por sensores termovelocimétricos para a sala dos servidores do data center, tipo VESDA, ou equivalente; possuir dispositivos de detecção precoce de incêndio pela análise do superaquecimento de cabos ou hardwares que sejam de maior sensibilidade que os tradicionais detectores de fumaça;
- Possuir sistema de detecção de incêndio por sensores termovelocimétricos para os ambientes de servidores e de armazenamento de dados;
- Possuir os componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.

2.6.15. O Data Center que alocará o ambiente computacional da USCS e deverá possuir os seguintes requisitos de segurança física:

- Disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;
- Mecanismos efetivos de controle de entrada e saída de pessoas que acessem e façam uso do IDC, bem como de registros passíveis de posterior pesquisa;
- Capacidade de cadastro remoto de usuários para acesso ao data center;
- Deverá possuir a capacidade de cadastro de novo usuário local com permissão do administrador;
- Acesso ao local através de leitura biométrica;
- Possuir alerta por SMS e e-mail em tempo real de acesso ao ambiente;
- Arquivar as imagens gravadas pelas câmeras de vídeo de segurança por pelo menos 30 (trinta) dias;
- O Datacenter deverá possuir vigilância patrimonial 24 horas por dia, 7 dias por semana, 365 dias por ano, permitindo apenas a entrada de pessoas autorizadas e devidamente identificadas;
- Possuir metodologia para classificação e controle de ativos e de acessos ao ambiente do Datacenter;
- Acondicionar equipamentos e mídias geradas no ambiente do Datacenter, livres de riscos físicos;
- Possuir rígido controle de acessos aos equipamentos do Datacenter, mesmo por pessoas credenciadas pela Contratante;
- Disponibilizar mecanismos efetivos de controle de entrada e saída de pessoas, que acessam ou façam uso do Datacenter, com leitores biométricos ou cartões magnéticos individuais;
- Possuir travas eletrônicas que, de acordo com a política de segurança estabelecida para o Datacenter, a dívida em regiões com níveis de restrição diferenciados;
- Possuir sistema de detectores de movimento no ambiente.

2.7. COMUNICAÇÃO COM A INTERNET E REDUNDANCIA

2.7.1. Deverá ser disponibilizado pela contratada 1 link de internet para gerenciamento de no mínimo de 50MB dedicado.

2.7.2. Será fornecido um link da REDNESP (ANSP), que deverá ser instalado e configurado conforme as especificações técnicas definidas no **Item 2.7**.

2.7.3. A CONTRATADA deverá disponibilizar no data center ofertado toda a estrutura para receber o link da CONTRATANTE que deverá ser interligado com o link disponibilizado pela FAPESP gratuitamente para acesso à internet, sendo, portanto, um ponto da rede de acesso da Rednesp (ANSP);

2.7.4. É de total responsabilidade da Contratada toda a infraestrutura necessária para realizar a interligação da unidade e data center destacado.

2.7.5. A Contratada deverá interligar o ambiente de nuvem privada da Contratante com a rede da Rednesp (ANSP).

2.7.6. A Contratada deverá prover a conectividade entre a sala de cross do Data Center e o cage da Rednesp (ANSP), bem como o rack ou cage (gaiola) onde estarão hospedados os servidores virtuais da Contratante.

2.7.7. A Contratada deverá interligar a unidade localizada na Avenida Goiás, 3400, Barcelona, São Caetano do Sul, São Paulo com o ambiente em cloud hospedado através de fibra ótica, com velocidade mínima de 1Gb.

2.7.8. A navegação na internet da unidade citada acima deverá ser através do link disponibilizado pela FAPESP, utilizando a interligação de fibra ótica, conforme item anterior.

2.8. BACKUP DO AMBIENTE COMPUTACIONAL

2.8.1. Toda a estrutura computacional em nuvem deverá ter backup diário.
2.8.2. O Backup deverá ser executado todos os dias e a cada 4 (quatro) horas.
2.8.3. Por dia o backup deverá ter 6 pontos de restauração.
2.8.4. O backup mensal deverá ter no mínimo 180 pontos de restauração.
2.8.5. A retenção do backup deverá ser de no mínimo por 1 (um) ano.
2.8.6. O licenciamento da solução deverá cobrir a solução de Armazenamento e Compartilhamento de arquivos em Windows, presente neste documento, pelo período do contrato;
2.8.7. A solução deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução, incluindo retorno (rollback) de réplicas e replicação até a infraestrutura virtualizada.
2.8.8. O software de backup deverá cobrir pelo menos 30 máquinas virtuais.
2.8.9. A solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.
2.8.10. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização Hyper-V, conforme Contratada.
2.8.11. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes.
2.8.12. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto.
2.8.13. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
2.8.14. Deverá prover a deduplicação e compressão das máquinas virtuais diretamente e durante a operação de backup.
2.8.15. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.
2.8.16. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.
2.8.17. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.
2.8.18. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreio de blocos modificados" (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
2.8.19. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:

- Diretamente através de Storage Area Network (SAN);
- Diretamente do storage, através do hypervisor I/O (Virtual Appliance);
- Mediante uso da rede local (LAN);
- Diretamente do snapshot do storage onde os dados das VMs estejam armazenados; (para Netapp, HPE 3Par ou EMC VNX).

2.8.20. Deverá proporcionar um controle centralizado de implementação distribuída, para isso deverá incluir uma console web, integrada ou não, que possibilite uma visão consolidada de sua arquitetura distribuída e conjunto de múltiplos servidores de proteção (backup), relatórios centralizados, alertas consolidados e restauração de autosserviço de máquinas virtuais no nível de sistema de arquivos (granular), com delegação de permissões sobre máquinas virtuais individuais.
2.8.21. Deverá poder manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço.
2.8.22. Deverá contar com tecnologia de deduplicação também para o ambiente de máquinas virtuais para gerar economia de espaço de armazenamento no repositório de backups sem a necessidade de hardware de terceiros (appliance deduplicadora).
2.8.23. Deverá proporcionar proteção quase contínua de dados (near-CDP), permitindo a minimização dos Objetivos de Pontos de Recuperação (RPO).

2.8.24. Deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do arquivo de backup, armazenado no repositório de backup de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do backup, os quais obrigatoriamente deverão estar "deduplicados" e também "comprimidos".
2.8.25. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.
2.8.26. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.
2.8.27. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar
2.8.28. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup.
2.8.29. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
2.8.30. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle.
2.8.31. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.
2.8.32. Deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.
2.8.33. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2010 sp1, 2013 e superiores, possam recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma.
2.8.34. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft Active Directory, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
2.8.35. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, tais como Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
2.8.36. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2010, sem a necessidade de agentes. (recuperação granular).
2.8.37. Deverá incluir ferramentas de recuperação de elementos individuais para Microsoft Exchange 2010-SP1 em diante, sem que seja necessário inicializar a máquina virtual a partir do backup e que possa ser extraído a frio (ex. mensagens, tarefas, contatos, etc.) e sem requerer infraestrutura intermediária (staging), fazer busca rápidas no servidor de e-mail
2.8.38. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, gerando confiabilidade de 100% na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.).
2.8.39. Deverá permitir criar uma cópia da máquina virtual de produção, para criação de ambiente de homologação, teste, QA, etc; em qualquer estado anterior para a resolução de problemas, provas de procedimentos, capacitação, entre outros. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only).
2.8.40. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO3 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS.
2.8.41. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.

2.8.42. Deverá ser fornecida com a funcionalidade de acelerar a rede "WAN" para geração de cópia ou replicação das máquinas virtuais, sem utilização de agentes, nem configurações de rede especiais.

2.8.43. Deverá incluir suporte para VMware vCloudDirector com visibilidade integrada da infraestrutura vCD no console de backup, fazendo backup de meta-dados e dos atributos associados com vApps e VMs, permitindo a recuperação diretamente ao vCD.

2.8.44. Deverá incluir um plug-in para VMware vSphere Web Client, afim de permitir o monitoramento da infraestrutura de backup diretamente do vSphere Web Client, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup.

2.8.45. Deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:

- Microsoft Active Directory Server 2008 R2 em diante
- Microsoft Exchange Server 2010-SP1 em diante;
- Microsoft SQL Server 2008 SP4 em diante;
- Microsoft Sharepoint 2010 em diante;
- Oracle Database 11g, 12c, 18c, 19c e 21c.

2.8.46. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados.

2.8.47. Deverá regular de forma dinâmica e parametrizável, a exigência sobre os sistemas protegidos, de forma tal, que se possa definir limites de utilização de performance em discos para diminuir o impacto na infraestrutura de produção, durante as atividades de backup.

2.8.48. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência.

2.8.49. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação.

2.8.50. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.

2.8.51. Deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de backup que esteja alojado em um provedor de serviços na nuvem (backup ou replicação na nuvem - cloud providers).

2.8.52. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas;

2.8.53. Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:

- Microsoft Windows;
- Linux;
- Pastas compartilhadas;
- Appliances de duplicadoras.

2.8.54. Suportar servidores proxy de backup virtuais ou físicos para backup de máquinas virtuais;

2.8.55. Deve estar homologado para o Oracle Database 11g e 12g nos sistemas operacionais Windows ou Linux sem a necessidade de instalação de agentes;

2.8.56. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;

2.8.57. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a Universidade Municipal de São Caetano do Sul se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem incorrer em nenhum ônus adicional decorrente dessa decisão.

2.8.58. Além do armazenamento em nuvem, o backup deverá ter uma unidade com imutabilidade, realizando o armazenamento e podendo ser solicitado a qualquer momento.

2.8.59. A solicitação de recuperação do backup não poderá ter custos adicionais por taxa de transferência.

2.9. INSTALAÇÃO E CONFIGURAÇÃO DO AMBIENTE COMPUTACIONAL

2.9.1. Deverão ser instalados e configurados os itens lógicos seguindo os padrões e melhores práticas recomendadas conforme critérios definidos pela contratante;

2.9.2. O ambiente computacional deverá ser capaz de acomodar até **30 máquinas virtuais** com o sistema operacional, sendo de responsabilidade da Contratante fornecer o licenciamento.

2.9.3. Os recursos alocados para a virtualização deverão ser apresentados pela Contratante não ultrapassando o limite contratado.

2.9.4. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

2.9.5. Prestar todos os esclarecimentos que lhe forem solicitados, atendendo prontamente a quaisquer reclamações;

2.9.6. Entregar toda mão de obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;

2.9.7. Os equipamentos de firewall do data center em cloud devem ser configurados em alta disponibilidade, no modo ativo/ativo, dois equipamentos funcionando simultaneamente e em caso de falha o outro deverá assumir a operação;

2.9.8. Deverá migrar ou executar configurações similares às configurações atuais implementadas no ambiente em cloud, atualmente em produção.

2.9.9. O ambiente deverá ser entregue com os softwares e atualizações mais recentes disponibilizados pelo fabricante tanto quanto, ambiente de conectividade via firewall, sistemas operacionais, firmwares e drives para que se obtenha total compatibilidade.

2.9.10. A empresa quando contratada deverá elaborar um plano de implantação junto a Universidade Municipal de São Caetano do Sul USCS, contendo descrição de atividades a serem desenvolvidas, relatórios e diagramas com dados relevantes para efeito decisório, responsáveis pelas atividades, cronograma de implementação, compondo o documento denominado “Projeto Executivo” tendo a visibilidade completa do projeto e seus status evolutivos. O documento deve ser entregue para a contratante antes do início da instalação, em até 10 dias úteis a partir do 1º dia útil subsequente a assinatura do contrato. A Diretoria de TI da USCS analisará o documento e dará o aceite em um prazo máximo de 02 dias úteis. Havendo necessidade de adequações a empresa terá um prazo máximo de 02 dias úteis para apresentar o projeto readequado, que será reavaliado pela Diretoria de TI para aprovação, em um prazo máximo de 01 dia útil.

2.9.11. Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno das melhores práticas recomendadas pelos fabricantes dos produtos e softwares envolvidos. Tal conhecimento deverá ser evidenciado por meio de certificações, emitidas pelos respectivos fabricantes ou entidades reconhecidas, que comprovem a qualificação técnica dos profissionais responsáveis pela implantação da solução;

2.9.12. As senhas configuradas no ambiente durante a instalação deverão ter requisito mínimo de 08 (oito) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;

2.9.13. Os profissionais técnicos da Contratada quando em serviço na Universidade Municipal de São Caetano do Sul deverão apresentar documento de identificação oficial com foto, previamente comunicados pela empresa e uniformizados;

2.9.14. A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente.

2.9.15. Deverá ser apresentado catálogo oficial, contendo as especificações técnicas dos produtos, bem como a camada de serviços ofertados para verificação técnica do responsável pela contratação.

2.10. SISTEMA DE SEGURANÇA CIBERNETICA

2.10.1. Requisitos técnicos da solução de segurança com inteligência artificial para detecção e resposta estendida a incidentes na camada de proteção nos servidores deverá ser totalmente compatível com a estrutura *in cloud*.

2.10.2. A contratação da prestação dos serviços e a disponibilização da ferramenta deverão atender integralmente aos normativos emitidos pelos órgãos fiscalizadores e de controle competentes, em especial ao disposto na Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

2.10.3. A plataforma deve contar com agentes da Inteligência Artificial para auxiliar em toda a etapa da investigação.

2.10.4. A plataforma deve disponibilizar comunicação direta por texto com os agentes da Inteligência Artificial.

2.10.5. A solução deve ser concebida nativamente sobre uma arquitetura distribuída de múltiplos agentes de software autônomos, sendo no mínimo 6 agentes de IA, não podendo ser um mero agregado de ferramentas de terceiros.

2.10.6. Cada agente deve ser um processo de baixo impacto (low footprint) em termos de consumo de CPU e memória, capaz de operar de forma contínua no ativo (servidor, computador, etc.) sem degradar sua performance.

2.10.7. Os agentes de IA utilizaram o seu conhecimento para orquestrar atividade nos ativos, de acordo com a demanda as atividades serão auditadas, executadas e documentadas.

2.10.8. A IA e os seus agentes devem ser o motor de orquestração central, utilizando um modelo de Gráfico de Conhecimento (Knowledge Graph) para mapear dinamicamente e em tempo real os relacionamentos entre todos os ativos do ambiente (identidades, dispositivos, aplicações, dados, vulnerabilidades, etc.) e organizá-los em um contexto de dados no qual os agentes tenham a capacidade de personalizar a interação do usuário, diminuir a complexidade, aumentar a qualidade e a produtividade.

2.10.9. A plataforma deve ser capaz de, a partir da análise deste gráfico, inferir cadeias de ataque (Cyber Kill Chains) complexas e multivetoriais, correlacionando eventos de baixa relevância que, isoladamente, não seriam considerados ameaças.

2.10.10. A resposta a incidentes deve ser dinâmica e contextual, baseada nas inferências do motor cognitivo, superando a execução de fluxos de trabalho estáticos e lineares.

2.10.11. A plataforma deve disponibilizar durante a navegação, interação com a Inteligência Artificial e acesso aos dados investigados.

2.10.12. A plataforma deve utilizar diferentes agentes da Inteligência Artificial para investigação de endpoints, alertas e Inteligência de ameaças.

2.10.13. A inteligência Artificial deve ser capaz de buscar todos os endpoints cadastrados, alertas abertos e vulnerabilidades identificadas na interação por texto e o resultado deve ser retornado em tela.

2.10.14. Os agentes de Inteligência devem ser capazes de correlacionar todos os dados coletados, analisar e fornecer um parecer investigativo sobre quais ações foram e/ou devem ser realizadas.

2.10.15. Deve usar um modelo matemático gerado a partir de aprendizado de máquina para comparar diferentes características de um arquivo executável, de forma estática, para determinar se ele é malicioso.

2.10.16. A plataforma deve ser capaz de detectar vazamentos de dados relacionados à Contratante, indicando o tipo de dado exposto e as datas que ocorreram.

2.10.17. A plataforma através dos agentes da Inteligência Artificial deve ser capaz de reclassificar a pontuação de risco da ameaça de acordo com a técnica explorada e a classificação do ativo;

2.10.18. A plataforma deve ser capaz de se integrar a aplicações e equipamentos da Contratante para enriquecer a detecção e resposta estendida em tempo real;

2.10.19. A proteção deve estar disponível para os sistemas operacionais Windows, Linux e MacOS.

2.10.20. Prevenção de ameaças baseada em comportamento para análise dinâmica de processos em execução.

2.10.21. Prevenção de exploração por técnicas conhecidas de exploits.

2.10.22. Prevenção de exploração baseada em kernel.

2.10.23. Prevenção de ameaças com base em inteligência de ameaças, como hash de arquivos.

2.10.24. Integração automatizada com um serviço de prevenção de malware, baseado em nuvem do próprio fabricante.

2.10.25. A solução deve prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros.

2.10.26. A solução deve ser compatível, no mínimo, com os seguintes sistemas operacionais e distribuições:

- Windows;

- Ubuntu;
- Oracle Linux;
- RedHat.

2.10.27. A solução deve incluir na análise de execução, no mínimo, as seguintes características:
- Táticas e técnicas de acordo com o modelo de ameaças MITRE ATT&CK;
- Caraterísticas comportamentais suspeitas;
- Detalhes do arquivo como nome, hash, tamanho, tipo;
- Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
- Leitura e escrita de arquivos em disco;
- Leitura e alteração de chaves de registro.

2.10.28. Detalhes de processos iniciados durante a execução.
2.10.29. Atualizações transparentes do mecanismo de detecção de ameaças.
2.10.30. Proteção contra malware, ransomware e ataques sem arquivo.
2.10.31. Identificação e prevenção de tentativas de escalonamento de privilégios ao nível de Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux.
2.10.32. Deve permitir gerar alertas das soluções integradas.
2.10.33. Deve permitir a consulta de eventos de forma integrada.
2.10.34. Os usuários locais da solução devem ter uma política de senha que permita, no mínimo as seguintes configurações, alteração no primeiro login e identificação de complexidade de senha.
2.10.35. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless).
2.10.36. No caso de detecção de um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos.
2.10.37. A solução deve disponibilizar o rastreio de detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências.
2.10.38. A solução deve disponibilizar o rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante.
2.10.39. A solução deve disponibilizar o rastreio de tentativas de roubo de credenciais e\ou tentativa de acessos indevidos a recursos chave do sistema operacional.
2.10.40. Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa artefatos, destacando rapidamente índices de comprometimento já conhecidos.
2.10.41. Gerenciamento unificado e centralizado de todas as funções na mesma console de, bem como a instalação e atualização dos agentes.
2.10.42. A solução deve possuir o recurso de autenticação, por usuário e senha, integrado a sistemas de e-mail, como o do Google (G-Suíte) ou da Microsoft (Office 365) para autenticar utilizando o método SSO (Single Sign On).
2.10.43. Detecção de comprometimento: vírus, malware, backdoors, hosts em comunicação com sistemas infectados por botnet, serviços da Web vinculados a conteúdo malicioso.
2.10.44. Frequência de atualização, personalizável por dia, semana ou mês.
2.10.45. Varredura em tempo real de arquivos (gravação, renomeio e leitura) e de processos em memória.
2.10.46. Monitoramento em tempo real para captura de malwares que são executados em memória sem a necessidade de escrever em arquivo.
2.10.47. Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise comportamental, realizado por inteligência artificial.
2.10.48. Solução única para proteção contra malwares e ransomware, com a capacidade de coletar dados de sistemas operacionais e de rede para detecção de eventos maliciosos, sem a obrigatoriedade de criação e ativação de regras manualmente.
2.10.49. A solução deve permitir instalação silenciosa do agente, em sistemas operacionais Windows, através de pacotes MSI e executável EXE.
2.10.50. A solução deverá ser capaz também de analisar ameaças, sem o uso de assinaturas, fazendo esta análise por comportamento.
2.10.51. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações.

2.10.52. A solução deve suportar nativamente a integração com terceiros, sem a necessidade de instalação de recursos adicionais para receber eventos de múltiplas fontes de origem.
2.10.53. A solução deve disponibilizar, informações sobre o número de dispositivos que possuem o agente instalado e a versão do agente.
2.10.54. A solução deve ser capaz de monitorar e-mail e domínio para identificar vazamento de dados.
2.10.55. Requisitos de detecção e resposta do agente
2.10.56. A solução não deve ter limitação para recebimento de eventos.
2.10.57. A comunicação entre agente e plataforma deve acontecer através do protocolo TCP porta 443;
2.10.58. O agente deve permitir a sua instalação em sistema operacional Linux Ubuntu 24.04 ou superiores.
2.10.59. A solução deve utilizar criptografia para conexão entre agente e plataforma, no mínimo, TLS 1.3 com AES 256.
2.10.60. A solução deve utilizar criptografia nos dados enviados para a plataforma de gerenciamento, no mínimo, AES 256.
2.10.61. A solução deve utilizar algoritmos de aprendizado de máquina para identificar padrões e comportamentos suspeitos.
2.10.62. A solução deverá ser capaz de bloquear tanto ameaças conhecidas como também as desconhecidas.
2.10.63. O agente deve detectar e proteger o dispositivo mesmo offline.
2.10.64. O agente deve receber atualizações de forma automática.
2.10.65. O agente deve receber as novas assinaturas de segurança em tempo real.
2.10.66. A solução deve utilizar detecção de ameaças por meio de dados e padrões baseados em comportamentos, que se utilizam de motores baseados em aprendizado de máquina para averiguação de arquivos.
2.10.67. O agente deve possuir a funcionalidade de inteligência contra malware.
2.10.68. O agente deve possuir a funcionalidade de inteligência contra ransomware.
2.10.69. O agente deve possuir a funcionalidade de bloqueio de indicadores de comprometimento.
2.10.70. O agente deve disponibilizar na sua interface, os seguintes dados:
2.10.70.1. Nome do usuário logado;
2.10.70.2. Nome do host;
2.10.70.3. Informações de sistema operacional (Build, Plataforma);
2.10.70.4. Estado do equipamento (Online ou Offline);
2.10.70.5. Última data comunicação com a console de gerenciamento;
2.10.70.6. Informações relacionadas à rede (IP, DNS, DHCP).
2.10.71. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela contratada.
2.10.72. A solução deve operar em tempo real, monitorando e bloqueando as ameaças.
2.10.73. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes.
2.10.74. A solução deve fornecer a capacidade de executar análises de estações de trabalho/servidores sem a necessidade de interagir com o usuário. Essa capacidade deve ser centralizada e transparente para o usuário.
2.10.75. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger e atualizar.
2.10.76. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho.
2.10.77. A solução deve ser capaz de fazer análise avançada e utilizar algoritmos de aprendizado de máquina, mesmo que sem conexão ao servidor de gerenciamento.
2.10.78. Consulta APIs: Capacidade de extrair dados de segurança e eventos para integração, utilizando os protocolos SSH, HTTP, SNMP e Syslog em todos os itens fornecidos dentro da solução proposta.
2.10.79. A solução deve disponibilizar um agente instalável e compatível com sistemas operacional, Windows, Linux e MacOS. Com a capacidade de detectar, coletar e enviar a plataforma, comportamentos maliciosos de aplicações que estão sendo executadas no sistema operacional.

2.10.80. A solução deve disponibilizar um coletor com capacidade de executar consultas de coleta de eventos e detecção de ação maliciosas em suas integrações, mesmo se houver indisponibilidade de conectividade.
2.10.81. Atualizações regulares e automáticas de binários e base de dados de segurança.
2.10.82. O agente deve ser compatível com o sistema operacional Linux Ubuntu 24.04 ou superiores.
2.10.83. A solução deve suportar a integração baseada em agente e autenticação.
2.10.84. A solução deve permitir o recebimento de eventos por múltiplos coletores.
2.10.85. A solução deve identificar os eventos por integração e agente.
2.10.86. A solução deve permitir a classificação de severidade, quando cadastrado o dispositivo.
2.10.87. Quanto ao armazenamento
2.10.87.1. A solução deve prover no mínimo 2TB de armazenamento para retenção dos eventos coletados e normalizados pela solução, sem custo adicional ou necessidade de fornecimento de hardware para armazenamento pela Contratante.
2.10.87.2. O evento armazenado pela solução, bem como hardware necessário para tal, é de responsabilidade da empresa Contratada em armazenar em Datacenter.
2.10.87.3. Solução deve ter a capacidade de permitir que a Universidade USCS modifique o período de armazenamento de eventos de Windows, Linux e Firewall de forma independente e através de plataforma gráfica disponibilizada pela solução proposta pela empresa Contratada.
2.10.88. Quanto a Relatórios e Dashboards
2.10.88.1. Visualização de Dados.
2.10.88.2. Painéis de controle para visualização em tempo real de incidentes e status de segurança;
2.10.88.3. Relatórios sobre incidentes, tendências de segurança e desempenho do sistema, exportando em formatos pdf, csv e html;
2.10.88.4. A solução deve ter capacidade de enviar relatórios através dos protocolos SMTP, HTTP, SFTP e ter integração com soluções de colaboração.

2.11. MONITORAMENTO

2.11.1. O serviço de monitoramento deverá ser composto de tecnologia que seja totalmente apartada do ambiente computacional e de servidores da Universidade Municipal de São Caetano do Sul.
2.11.2. A empresa Contratada deverá monitorar o ambiente 24x7 (vinte e quatro horas por dia, sete dias por semana), conforme descrito nesse documento;
2.11.3. O monitoramento deverá ter vigência de 24 (vinte e quatro) meses;
2.11.4. A disponibilidade e monitoramento deverá ocorrer por 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana;
2.11.5. Deverá ter **SLA** de disponibilidade da console de gerenciamento de no mínimo **99,982%**;
2.11.6. A solução de monitoramento deverá estar hospedada em Datacenter com a classificação mínima de **Tier III**;
2.11.7. A solução de monitoramento deverá ter portal de acesso de visualização WEB disponibilizada para a Diretoria de Tecnologia da Informação da Universidade USCS;
2.11.8. Deverá ser capaz de enviar alertas de alteração de status de sensores através de correio eletrônico;
2.11.9. Possuir pelo menos os seguintes status para os sensores de monitoramento: Estado normal, estado de alerta e estado de erro;
2.11.10. Possuir a possibilidade para criação de interface WEB com mapa de distribuição de arquitetura com o monitoramento, podendo ter acesso público e/ou autenticado através de contas de usuários internas da solução de monitoramento;
2.11.11. O monitoramento deverá ser compatível com os principais serviços de nuvem pública;
2.11.12. O sistema de monitoramento deverá contar com aplicativo de administração instalável e homologado para o sistema operacional Linux;
2.11.13. A solução de monitoramento deverá abrir chamado de maneira automática junto a USCS, após a alteração de um sensor para o estado de alerta ou erro;
2.11.14. A ferramenta de monitoramento deve ser capaz de realizar a coleta de dados de diversos dispositivos e sistemas, incluindo servidores, dispositivos de rede e aplicações. Os principais requisitos incluem:
2.11.15. A ferramenta deverá realizar a coleta de métricas de desempenho, como uso de CPU, memória, espaço em disco, latência de rede, e status de serviços. A coleta será feita de forma agendada

ou por meio de eventos de trap (alerta gerado pelo próprio dispositivo) onde será necessário que os dispositivos entreguem as informações através do protocolo SNMP.

2.11.16. A ferramenta deverá ser capaz de monitorar diversos tipos de hosts, com a possibilidade de utilização de agentes para coleta de dados, bem como monitoramento sem agentes para dispositivos de rede e outros dispositivos que não possuam um agente instalado.

2.11.17. A ferramenta deve ser capaz de gerar alertas e notificações de forma automatizada, baseados em eventos ou métricas predefinidas. As notificações poderão ser enviadas por e-mail ou outras integrações, como sistemas de gerenciamento de incidentes. A ferramenta deverá também permitir a definição de escalonamentos de alertas e ações automáticas, como reiniciar um serviço ou executar comandos específicos em resposta a incidentes quando houver a disponibilidade de conexão via SSH.

2.11.18. A ferramenta deverá possuir uma interface gráfica baseada na web que permita a visualização de dados em tempo real, com dashboards personalizáveis. A interface deve ser intuitiva, acessível e permitir a criação de relatórios gerenciais com informações detalhadas sobre a saúde e o desempenho da infraestrutura.

2.11.19. A plataforma deverá garantir segurança através de autenticação de usuários e controle de permissões, permitindo a definição de diferentes níveis de acesso. A comunicação entre a ferramenta e os dispositivos monitorados deverá ser criptografada para garantir a proteção dos dados durante a transmissão.

2.11.20. A solução deverá ser escalável, permitindo seu uso tanto em ambientes de pequeno porte quanto em grandes infraestruturas corporativas, com a possibilidade de monitoramento de milhares de dispositivos simultaneamente. Para grandes ambientes, deverá ser possível utilizar proxies para distribuição do monitoramento.

2.11.21. A ferramenta deve permitir a geração de relatórios periódicos, tais como dia anterior, semana anterior, mês anterior, ano anterior e a realização de análises de tendências para prever possíveis falhas ou pontos de saturação da infraestrutura. A análise histórica deverá ser capaz de identificar padrões e comportamentos anormais através do armazenamento dos históricos no recurso tecnológico que a Contratada deverá entregar com o serviço de monitoramento.

2.11.22. A ferramenta deve ser compatível com sistemas operacionais Linux e Windows, e permitir a instalação em ambientes físicos ou virtuais, de acordo com a necessidade do cliente.

2.11.23. A ferramenta deverá utilizar uma base de dados para armazenar as informações coletadas, com a possibilidade de utilização de bancos de dados open-source, como MySQL, PostgreSQL ou similares.

2.11.24. A solução deverá permitir integrações com outras plataformas de TI, como sistemas de gerenciamento de incidentes, plataformas de visualização de dados, e outras ferramentas de automação e análise de infraestrutura.

2.11.25. A implementação da ferramenta será realizada em etapas, incluindo a instalação do proxy através do recurso tecnológico, configuração e personalização conforme os requisitos específicos da infraestrutura de TI.

2.11.26. Deverá ser possível a geração de relatórios com dados de tabela e gráficos para quaisquer sensores que compõem a solução;

2.12. RELÁTORIOS

2.12.1. Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, contendo:

2.12.2. Relatório de Chamados (referente ao serviço descrito nesse lote):

2.12.3. Categoria do chamado;

2.12.4. Usuário;

2.12.5. Ativos relacionados;

2.12.6. Data de abertura e fechamento;

2.12.7. Status;

2.12.8. Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):

2.12.9. Disponibilidade;

2.12.10. Consumo de hardware (CPU, memória, disco, consumo de banda);

2.12.11. Alertas e erros;

2.13. SUPORTE TÉCNICO

2.13.1. Os serviços de suporte técnico especializado, deverão contemplar toda a solução e infraestrutura de segurança contidas neste Termo de Referência.

2.13.2. A Contratada deverá administrar e monitorar o serviço de segurança descrito nesse documento;

2.13.3. A USCS poderá abrir chamados de manutenção através de chamada telefônica para número com DDD (11), central de atendimento via navegador (WEB) e correio eletrônico sem a necessidade prévia consulta e/ou qualquer liberação por parte da Contratada.

2.13.4. O atendimento técnico remoto deverá ocorrer 24 horas por dia.

2.13.5. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas de hardware e/ou software.

2.13.6. Toda falha e indisponibilidade no ambiente ocasionado por falhas físicas nos equipamentos (hardware) será de plena responsabilidade da empresa Contratada.

2.13.7. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos.

2.13.8. Será de responsabilidade da Contratada manter o pleno funcionamento das políticas de segurança da solução.

2.13.9. Deverá monitorar diariamente, os relatórios de segurança gerados ao concluir as tarefas, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da Contratada efetuar correção ou ajuste técnico para a normalização dele, garantindo o pleno funcionamento da solução;

2.13.10. A empresa Contratada deverá ser responsável por executar as restaurações do ambiente.

2.13.11. A empresa Contratada se responsabilizará pelas despesas com material de escritório, reprodução de documentos (cópias, etc.) e materiais diversos, que forem necessários à execução dos serviços de manutenção dos serviços e pelos seus profissionais;

2.13.12. A Contratada deverá realizar atendimentos remotos à equipe de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul, a partir de solicitações recebidas dos técnicos ou do gestor do instrumento de contrato a ser celebrado com a empresa vencedora do certame, via sistema de atendimento, telefone ou correio eletrônico;

2.13.13. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados;

2.13.14. Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências;

2.13.15. Manter o ambiente de segurança sempre atualizado em com as melhores práticas aplicadas;

2.13.16. A Contratada deverá garantir que os profissionais designados para atendimento técnico serão capacitados;

2.13.17. A garantia de tempo de resposta será realizada conforme critérios de prioridades elencados no quadro imediatamente abaixo:

Classe	Descrição	Início do Atendimento em até
1	Serviço indisponível	1 hora
2	Suporte técnico de maior impacto	4 horas
3	Suporte técnico com menor impacto	8 horas
4	Manutenção preventiva	Programada

2.13.18. O acordo de nível de serviço **(SLA)** para suporte técnico deverá obedecer ao seguinte escopo:

PRIORIDADE	DESCRIÇÃO
1 (Emergencial)	O serviço está fora de operação ou há um impacto crítico nas operações.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações que sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

2.13.19. As horas para primeiro atendimento e resolução de incidentes são horas corridas e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.
2.13.20. Caso seja identificado que o Serviço de Segurança se encontra indisponível por causa de soluções de terceiros, link de internet, indisponibilidade de switch, energia elétrica, roteadores, firewall, problemas de hardware/infraestrutura de TI ou qualquer serviço que interligue as unidades, será de responsabilidade da Contratada em realizar a detecção e resolução do problema.
2.13.21. A empresa Contratada deverá disponibilizar e gerenciar os atendimentos técnicos da USCS através de portal de gerenciamento de atendimentos com acesso a partir de navegador web;
2.13.22. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central;
2.13.23. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;
2.13.24. A Contratada deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento;
2.13.25. A Contratante deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail;
2.13.26. O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da empresa Contratada, sendo essa responsável por sua atualização e manutenção;
2.13.27. A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;
2.13.28. O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;
2.13.29. A Contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela Contratante;
2.13.30. Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;
2.13.31. Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a USCS;
2.13.32. O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a Universidade;
2.13.33. Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;
2.13.34. A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";
2.13.35. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;
2.13.36. Deverá ser possível a criação de grupos de usuários na solução;
2.13.37. A solução a ser disponibilizada pela empresa Contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.
2.13.37.1. Relatórios Mensais, durante o período do contrato;
2.13.37.2. Relatório de Chamados;
2.13.37.3. Categoria do chamado;
2.13.37.4. Usuário;
2.13.37.5. Ativos relacionados;
2.13.37.6. Data de abertura e fechamento;
2.13.37.7. Status;
2.13.38. O suporte técnico deverá ter os seguintes canais de atendimento: Suporte telefônico, e-mail e sistema online de chamados, todos em português do Brasil.
2.13.39. A empresa Contratada deverá sempre disponibilizar versões mais recentes dos softwares sem ônus financeiro.

2.14. MANUTENÇÃO PREVENTIVA DA SOLUÇÃO CIBERNETICA

2.14.1. A manutenção preventiva será destinada a atualizar os componentes de software (atualização tecnológica), conforme definições nesse documento, e a realizar quaisquer operações que evitem uma parada total ou parcial da solução

2.14.2. A USCS, através de sua equipe técnica de Tecnologia da Informação, observará o desempenho do sistema contratado e, caso necessário, solicitará à Contratada a manutenção preventiva para viabilizar o melhor desempenho da solução.

2.14.3. A manutenção preventiva está inclusa no suporte técnico da solução, sendo prestada pela Contratada sem qualquer ônus adicional para a Universidade.

2.14.4. Durante a manutenção preventiva, a USCS deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta.

2.14.5. Durante o período de suporte técnico deverá ser realizada a atualização de qualquer outro software constituinte da solução para as versões mais recentes, sem ônus adicional imputado à Contratante.

2.14.6. A manutenção corretiva será destinada a remover erros ou falhas apresentadas pelos componentes de software da solução contratada.

2.14.7. Como erro ou falha entende-se a geração de resultado diferente do previsto. Para a resolução desses erros, é necessária a intervenção técnica especializada ou mesmo até a substituição de seus componentes por parte da Contratada.

2.14.8. A manutenção corretiva após o diagnóstico (determinação da origem da falha) deverá ser realizada por meio de ajustes, consertos ou substituição dos elementos que apresentam problemas, restabelecendo a solução suas condições normais de funcionamento ou operação, conforme as especificações do fabricante.

2.14.9. Entende-se como diagnóstico à compilação e análise de informações para definição da causa de um problema.

2.14.10. Entende-se como Recuperação da Disponibilidade a execução de atividades que permitem restabelecer o funcionamento da solução.

2.14.11. A comprovação de isenção de responsabilidade se dará pela apresentação de relatório técnico circunstanciado dos elementos da solução contratada, e pelas demais informações consideradas necessárias pela Contratada para embasar a justificativa.

2.14.12. Tomar todas as providências necessárias para que seus funcionários, representantes e/ou contratados observem os regulamentos, normas e instruções de segurança da informação e Comunicações pela Contratante, quando estiverem executando serviços.

2.14.13. A Contratada deve comprometer-se a manter informações confidenciais no mais estrito sigilo sobre todos os dados, configurações, processos, fórmulas, rotinas e quaisquer outros objetos que sejam disponibilizados, pela USCS à empresa Contratada, para a realização dos trabalhos. Compromete-se a não copiar, não usar em seu próprio benefício, nem revelar ou mostrar a terceiros, nem divulgar tais informações, no território brasileiro ou no exterior, sob pena prevista em lei. Só os representantes e prepostos, devidamente autorizados entre as partes, cuja avaliação das informações confidenciais seja necessária e apropriada, para os propósitos especificados em contrato, terão acesso às mesmas.

2.14.14. Prestar os esclarecimentos necessários para a Contratante, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.

2.14.15. Requisitos sociais, ambientais e culturais

2.14.16. Sistema e todos os seus módulos deve ser desenvolvido/disponibilizado de forma compatível para as características do Brasil quanto a aspectos de interface gráfica, linguagem, legislação, costumes, apresentação, funcionalidades, telas e relatórios. Deve também possuir manuais de usuário on-line, com possibilidade de impressão, e documentação técnica do software em idioma português do Brasil ou inglês.

ANEXO II - PROPOSTA COMERCIAL	
Pregão Eletrônico nº 26/2025	**Abertura 19/12/2025 às 9h**
Razão Social:	
Endereço Eletrônico:	
CNPJ:	**Inscrição Estadual:**
Endereço:	**nº**
Bairro:	**Cidade:**
CEP:	**Estado:**
Fone / Fax:	**e-mail:**
Informação para pagamento:	
Banco: **Agência número:**	**Conta Corrente número:**

Para efeito de precificação e apresentação de proposta de preços, o proponente deve considerar todos os requisitos exigidos no termo de referência (anexo I) para a solução proposta concernente ao lote em disputa.

Importante **Os intens neste anexo foram ordenados levando-se em conta a sequência observada na inserção da proposta comercial no sistema de pregão eletrônico da USCS.**

LOTE 01 - Serviço de Segurança de Rede - Firewall *As a Service*

Item	Solução	Fabricante	Descrição	Modelo /Tipo	Cron. Pag.	Valor Unitário (em reais)	Valor Total (em reais)
1	*Solução de Firewall as a Service do **tipo 02.***		*Fornecimento de 2 Firewalls de próxima geração em **1 (uma)** estrutura em alta disponibilidade sendo equipamentos configurados no formato **ativo/ativo** com inspeção profunda de pacotes, prevenção contra intrusões, filtragem de conteúdo, controle de aplicações, VPN segura, proteção contra malware e gerenciamento centralizado pelo período de **24 (vinte e quatro)** meses.*		*24 meses*		
2	*Solução de Firewall as a Service do **tipo 01**.*		*Fornecimento de 4 Firewalls de próxima geração distribuídos em **2 (duas)** estruturas em alta disponibilidade sendo equipamentos configurados no formato **ativo/ativo** com inspeção profunda de pacotes, prevenção contra intrusões, filtragem de conteúdo, controle de aplicações, VPN segura, proteção contra malware e gerenciamento centralizado pelo período de **24 (vinte e quatro)** meses.*		*24 meses.*		
3	*Solução de Firewall as a Service do **tipo 03.***		*Fornecimento de 6 Firewalls de próxima geração distribuídos em **3 (três)** estruturas em alta disponibilidade sendo equipamentos configurados no formato **ativo/ativo** com inspeção profunda de pacotes, prevenção contra intrusões, filtragem de conteúdo, controle de aplicações, VPN segura, proteção contra malware e gerenciamento*		*24 meses*		

			*centralizado pelo período de **24 (vinte e quatro)** meses.*				
4	*Serviço especializado em suporte técnico com atendimento local e remoto nos serviços de Next Generation firewall dos **tipos 1, 2 e 3.***	Não preencher	*Serviço de Suporte Técnico com Atendimento Local e Remoto para os equipamentos de next Generation firewall em conformidade com as especificações contidas no termo de referência.*	Serviço	*24 meses*		
5	*Serviço especializado em monitoramento com atendimento para os serviços de Next Generation firewall dos **tipos 1, 2 e 3.***	Não preencher	*Serviço de Monitoramento (Noc) para os equipamentos de next Generation firewall em conformidade com as especificações contidas no termo de referência.*	Serviço	*24 meses*		
6	*Serviço especializado em instalação do Next Generation firewall dos **tipos 1, 2 e 3.***	Não preencher	*Serviço de instalação, configuração de todas as funções do serviço de next Generation firewall e criação da documentação final do projeto incluindo:* • *Planejamento e Projeto Executivo;* • *Instalação Física;* • *Configuração Lógica e Alta Disponibilidade;* • *"As built" (diagramas, parâmetros, endereçamentos, políticas);* • *Relatórios de testes (pré/pós) e Termo de Aceite.*	Serviço	*01*		
						Valor Global do Lote (em reais)	

LOTE 02 – Serviço de Hospedagem em nuvem Privada para a Estrutura Computacional USCS – Data Center Hosting

Item	Solução	Fabricante	Descrição	Modelo /Tipo	Cron. Pag.	Valor Unitário (em reais)	Valor Total (em reais)
1	*Serviço de instalação configuração e documentação total do ambiente **em nuvem.***	Não preencher	*Serviço de Instalação e Configuração de toda a infraestrutura em nuvem, incluindo:* • *Planejamento e Projeto Executivo;* • *Provisionamento do ambiente de virtualização;* • *Conectividade e segurança;* • *Migração do ambiente;* • *Segurança, conformidade e controles operacionais;* • *Documentação as built + inventário lógico do ambiente;* • *Relatórios de atualização/compatibilidade e de testes (pré/pós-migração) e Termo de Aceite.*	*Serviço*	*01*		
2	*Serviço especializado de **hosting** para suportar o ambiente computacional.*	Não preencher	*Serviço de Data Center Hosting com infraestrutura redundante, alta disponibilidade, climatização controlada, segurança física e lógica, conectividade de alta performance.*	*Serviço*	*24 meses*		
3	*Serviço especializado de suporte técnico no ambiente computacional **em nuvem**.*	Não preencher	*Serviço de Suporte Técnico com Atendimento Remoto para a infraestrutura em nuvem.*	*Serviço*	*24 meses*		
4	*Serviço especializado de monitoramento no ambiente computacional **em nuvem.***	Não preencher	*Serviço de Serviço de Monitoramento (NOC) remoto para a infraestrutura em nuvem.*	*Serviço*	*24 meses*		
						Valor Global do Lote (em reais)	

Valor Global da Proposta (em reais)	

Observações:

1 - Declaro que os serviços, equipamentos e licenciamentos ofertados obedecem a todas as condições estabelecidas no Anexo I do **Pregão Eletrônico 26/2025**, responsabilizando-me, pela veracidade desta informação;

2 – O proponente declara total concordância com os termos do edital, da minuta de contrato e das demais disposições e condições nos Anexos da referida licitação, modalidade pregão em sua forma eletrônica;

3 - Declaro que os preços contidos na proposta comercial incluem todos os custos e despesas diretas e indiretas, tributos incidentes, taxa de administração, materiais, serviços, encargos sociais trabalhistas, seguros, lucros e outros necessários ao cumprimento integral do objeto deste Edital e seus Anexos.

5 – Prazos de execução e Vigência do Contrato, em conformidade com os itens 12 e 13 deste Edital.

6 – Do faturamento e do pagamento, em conformidade com o item 14 deste edital.

7 - Prazo de validade da proposta, não inferior a 60 (sessenta) dias corridos, contados da data fixada para apresentação da proposta na sessão pública.

_____, ____ de dezembro de 2025.
(Local e data)

_____
Nome e assinatura do responsável

ANEXO III
REDUÇÃO DE LANCES

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

CRITÉRIO DE JULGAMENTO E LANCE

O critério de julgamento adotado será o de menor preço por lote, conforme anexo II – Proposta Comercial.

O percentual efetivo deve obrigatoriamente ser considerado para aplicação em cada item que compõe a proposta de preços para cada lote disputado.

Os lances obedecerão ao fator de redução de 0,50% (meio por cento)

ANEXO IV
DECLARAÇÃO DE REGULARIDADE PERANTE O MINISTÉRIO DO TRABALHO
(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

Eu,_____(nome completo), representante legal da empresa _____(razão social), interessada em participar do Pregão Eletrônico nº 26/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declaro, sob as penas da lei, que, nos termos do artigo 63, Inciso III, da Lei 14.133/2021, a empresa licitante _____(razão social), encontra-se em situação regular perante o Ministério do Trabalho, no que se refere à observância do disposto no Inciso XXXIII do artigo 7° da Constituição Federal.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO V

DECLARAÇÃO DE CUMPRIMENTO DAS CONDIÇÕES DE HABILITAÇÃO

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

À

Reitoria da Universidade Municipal de São Caetano do Sul

São Caetano do Sul - SP

Ref.: Pregão eletrônico nº 26/2025

Prezados Senhores,

Pela presente, declaramos para efeito do cumprimento ao estabelecido no inciso I do artigo 63º da Lei Federal nº 14.133/2021, sob as penalidades cabíveis, que cumprimos plenamente os requisitos de habilitação exigidos neste Edital.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO VI

DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE PARA FRUIÇÃO DOS BENEFÍCIOS DA LEI COMPLEMENTAR Nº 123/2006 COM AS DEVIDAS ALTERAÇÕES INTRODUZIDAS PELAS LEIS COMPLEMENTARES FEDERAIS Nº 147/2014 E 155/2016, E LEI MUNICIPAL Nº 4.660/2008

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

_____(nome do licitante), com sede _____(endereço completo), inscrita no CNPJ sob o número _____, Declara, para fins do disposto na Lei Complementar nº 123/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e 155/2016, e Lei Municipal nº 4.660/2008 sob as sanções administrativas cabíveis e sob as penas da lei, que esta Empresa, na presente data, enquadra-se como:

(...) MICROEMPRESA, conforme inciso I do artigo 3º da Lei Complementar nº 123, de 14/12/2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e nº 155/2016 e, inciso I do artigo 5º da Lei Municipal nº 4.660/2008.

(...) EMPRESA DE PEQUENO PORTE, conforme inciso II do artigo 3º da Lei Complementar nº 123 de 14/12/2006, com as devidas alterações introduzidas pelas Leis Complementares Federais nº147/2014 e nº 155/2016 e, inciso II do artigo 5º da Lei Municipal nº 4.660/2008.

Declara, ainda, que a empresa está excluída das vedações constantes do § 4º do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006 com as devidas alterações introduzidas pelas Leis Complementares Federais nº 147/2014 e nº 155/2016 e, § 2º do artigo 5º da Lei Municipal nº 4.660/2008.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO VII

DECLARAÇÃO DE ATENDIMENTO ÀS NORMAS RELATIVAS À SAÚDE E SEGURANÇA NO TRABALHO

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

A_____(razão social), por seu(s) representante(s) legal(is), interessada em participar do Pregão Eletrônico nº 26/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que observa as normas relativas à saúde e segurança no Trabalho, para os fins estabelecidos pelo parágrafo único do artigo 117 da Constituição do Estado de São Paulo.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO VIII

DECLARAÇÃO DE CONDIÇÕES GERAIS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

A Licitante declara estar de ciente e de acordo com os termos estabelecidos neste Edital, bem como:

1. Que atende aos padrões tecnológicos para sistemas, aplicações, arquivos de dados e outras ferramentas, garantindo que adota e implementa todas as medidas organizacionais e técnicas de segurança exigidas pela Lei Geral de Proteção de Dados - Lei n 13.709, de 14 de agosto de 2018 e suas alterações, bem como manterá durante o prazo do Contrato, as medidas para proteção dos Dados Pessoais contra destruição indevida, compartilhamento irregular ou não autorizado, perda acidental, alteração, acesso ou divulgação irregulares e/ou qualquer forma de Tratamento inadequado ou ilícito dos Dados Pessoais que lhe forem compartilhados.

2. Que as medidas de segurança e proteção dos Dados Pessoais serão pelo menos iguais ou superiores a cumulativamente a qualquer regulamentação definida pela ANPD ou outro órgão governamental competente, bem como aos padrões do ramo da USCS.

3. Que se encontra plenamente capaz de cumprir com os termos e condições do presente Edital, conforme declarado no Anexo II – Proposta Comercial e que, na eventualidade de uma relevante alteração das normas aplicáveis às atividades de Tratamento de Dados Pessoais que tenha potencial de modificar sua conformidade legal e contratual notificará a USCS.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO IX

DECLARAÇÃO DE QUE SUA PROPOSTA ECONÔMICA CONSIDERA OS CUSTOS TRABALHISTAS

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

A_____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 26/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que sua proposta econômica compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal de 1988, nas Leis Trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega da proposta comercial, consoante participação no processo licitatório em referência.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO X

DECLARAÇÃO DE CUMPRIMENTO À EXIGÊNCIA DE RESERVA DE CARGOS

(Preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

Em cumprimento as determinações contidas no inciso IV do artigo 63 da Lei Federal 14.133/2021, a proponente licitante _____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 26/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que cumpre os requisitos legais pertinentes à habilitação social no que concerne à reserva legal de cargos para pessoas portadores de deficiência e para reabilitados da Previdência Social previstas na Lei Federal 8.213/1991.

_____, ____ de dezembro de 2025.
(Local e data)

_____
(Nome e assinatura do representante legal da Licitante)

ANEXO XI

DECLARAÇÃO DE QUALIFICAÇÃO TÉCNICA DO PROFISSIONAL QUE SERÁ ALOCADO NO PROJETO

(preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

A licitante _____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 26/2025, da Reitoria da Universidade Municipal de São Caetano do Sul - USCS, declara, sob as penas da lei, que dispõe de profissional técnico qualificado, consonante, especificamente com a necessidade técnica exigida para o projeto de implementação da infraestrutura de tecnologia para solução de segurança perimetral (Next Generation e Firewall), referenciada no lote 01, e/ou Serviço de Hospedagem em Nuvem (Data Center Hosting) referenciada no lote 02 e, cujo quantitativo satisfaz plenamente a demanda necessária para o pleno atendimento das exigências contidas no documento Termo de Referência do Edital - Anexo I.

_____, ____ de dezembro de 2025.
(Local e data)

_____
Nome e assinatura do representante legal da Licitante

ANEXO XII

DECLARAÇÃO DE QUALIFICAÇÃO DE CREDENCIADO JUNTO AO FABRICANTE DO EQUIPAMENTO

(preferencialmente em papel timbrado da licitante)

Pregão Eletrônico nº 26/2025
Processo de Compras nº 848/2025

A licitante _____(razão social), por seu representante legal, interessada em participar do Pregão Eletrônico nº 26/2025, da Reitoria da Universidade Municipal de São Caetano do Sul, ***especificamente em relação ao lote 01***, **declara**, sob as penas da lei, que detém a condição de parceiro credenciado junto ao fabricante cujo status lhes permite atuar como fornecedor na área de serviço de segurança de rede, ou, que é revendedor autorizado do fabricante, com capacidade para oferecer e fornecer suporte aos equipamentos efertados As a Service, bem como declara estar apto a realizar suas implantações, de acordo com as exigências contidas no termo de referência do edital.

_____, ____ de dezembro de 2025.
(Local e data)

_____
Nome e assinatura do representante legal da Licitante

ANEXO XIII

MINUTA DE CONTRATO Nº ___/2026 E TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE DE PROTEÇÃO DE DADOS PESSOAIS QUE ENTRE SI CELEBRAM A "UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL – USCS", E A EMPRESA " _____"

Aos _____ dias do mês de _____ do ano de 2026, a **Universidade Municipal de São Caetano do Sul - USCS**, por intermédio da Reitoria, inscrita no CNPJ sob nº 44.392.215/0001-70, sediada à Avenida Goiás, 3400, Bairro Barcelona - São Caetano do Sul - CEP 09550-051 – Estado de São Paulo, neste ato representada pelo Reitor o senhor _____, inscrito no Cadastro de Pessoa Física CPF, sob número 000.***.***-00, doravante denominada Contratante e, de outro lado, a empresa _____, inscrita no CNPJ sob nº _____, sediada à _____, nº _____ – Vila: _____ – _____ – CEP _____ – _____, neste ato representada na forma de seu contrato social, pelo _____, portador do Cadastro de Pessoa Física nº 000.***.***-00, doravante denominada Contratada, com fundamento na Lei Federal nº 14.133/2021, Lei Municipal nº 4660//2008, estando as partes vinculadas ao Processo de Compras 848/2025 Edital de Pregão Eletrônico nº 26/2025 e a proposta vencedora, assinam o presente contrato de fornecimento e serviços, obedecendo as seguintes disposições:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente instrumento contratual tem por objeto a contratação de empresa especializada para o fornecimento de infraestrutura e serviços de hospedagem em nuvem, bem como solução de segurança perimetral (Next Generation Firewall) para atendimento ao ambiente de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul, conforme condições e especificações constantes no edital e seus anexos.

1.2. A Contratada ficará obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco) por cento do valor inicial atualizado do contrato.

CLÁUSULA SEGUNDA - DOS PRAZOS

2.1. A Contratada deverá cumprir os seguintes prazos para a perfeita execução do instrumento contratual:

2.1.1. A contratada deverá cumprir o prazo estipulado de até 60 dias para o fornecimento dos equipamentos de firewall *as a service*, licenciamento, bem como a instalação e configuração relativas ao **lote 01**, a contar da aprovação do projeto executivo pelo gestor do contrato, cujo escopo remete às especificações contidas no termo de referência do edital;

2.1.2. Em relação ao **lote 02**, a contratada terá o prazo de 60 dias para migração das aplicações e base de dados legado, instalação e configuração dos equipamentos na nova estrutura computacional in cloud, contados a partir da aprovação do projeto executivo pelo gestor do contrato;.

2.1.3. A empresa deverá elaborar plano de implementação junto a Universidade USCS, nos termos dos subitens 1.11.10 e 2.9.10. aportados ao TR do edital, respectivamente para os lotes 01 e 02, compondo o documento nomeado "Projeto Executivo" em até 10 dias úteis, computados a partir do dia seguinte ao envio da ordem de serviços, cujo escopo remete às especificações contidas no Termo de Referência do edital.

2.1.4. Caso a ordem de serviço seja enviada por correspondência eletrônica, o prazo para entrega dos equipamentos, migração da base de dados legado, instalação e configuração da solução para quaisquer dos lotes contratados, independente do recebimento, inicia-se 24 (vinte e quatro) horas após sua expedição, ressaltando-se que o prazo deve iniciar em dia útil.

2.1.5. **Quanto ao serviço mensal de Hosting, Suporte Técnico, Manutenção, Monitoramento e Segurança de Rede**

2.1.5.1. Concluído a fase de estruturação que contempla a disponibilização física de equipamentos *as a service*, migração das aplicações e base de dados legado, acompanhados de sua respectiva instalação e configuração, distintamente para ambos os lotes, o gestor do contrato designado pela USCS terá o prazo máximo de até 5(cinco) dias para conferência e emissão do **Termo de Aceitação**. A partir de então, iniciar-se-á a prestação mensal dos serviços descritos acima, elencados sob a forma de solução integrada em cada lote correspondente.

2.1.5.1.1. Em particular, no que concerne ao lote 01, a implantação dos equipamentos *as a service*, bem como os serviços de instalação e configuração, dar-se-ão de modo parcial, de acordo com o cronograma a ser definido entre a Contratada e a gestão do instrumento de contrato da Universiidade USCS. Portanto, o termo de aceitação e consequentemente o pagamento por essa etapa de infraestrutura será paulatino, do mesmo modo a ativação dos serviços decorrentes de tal implantação (suporte técnico 24x7 e monitoramento NOC).

2.1.5.1.2. O cronograma de execução, notadamente relativo ao lote 01, deverá indicar de modo percentual a distribuição e execução dos serviços, considerando-se o dimensionamento e as respectivas unidades da Universidade USCS que integram o projeto, estabelecido no termo de referência do edital (item 1, “a”).

2.1.5.2. Quanto aos serviços de Segurança de Rede (lote 01), Data Center e Hosting (lote 02), bem como o serviço de suporte técnico, serviço de manutenção e monitoramento NOC no formato 24x7, dispostos em ambos os lotes, terão seu início computado para efeito de pagamento na data constante do termo de aceitação emitida pela gestão do instrumento contratual da USCS, respeitando-se a condição (*pró-rata - no sentido de proporcionalidade*) disposta no subitem 12.3. e seguintes do instrumento convocatório, para o primeiro pagamento, caso não se inicie no primeiro dia do mês.

2.1.5.2.1. Para efeito de pagamento relativa aos serviços descritos no subitem imediatamente anterior, deverá ser considerado o escopo de fornecimento e a distinção para cada um dos lotes contratados.

CLÁUSULA TERCEIRA – DA VIGÊNCIA DO CONTRATO

3.1. A Universidade Municipal de São Caetano do Sul firmará contrato de prestação de serviços de suporte técnico, manutenção e monitoramento (NOC) e segurança de rede (firewall *as a service*), consoante lote 01, assim como serviço mensal de suporte técnico, manutenção e monitoramento (NOC) referente a estrutura computacional em Data Center e Hosting, registrados nos termos definidos para o lote 02, por prazo de 24 (vinte e quatro) meses consecutivos e ininterruptos, contados a partir do recebimento da ordem de serviços, conforme disposto no subitem 2.1.4., podendo ser prorrogado por igual período, de comum acordo, desde que devidamente justificado e manifestado com antecedência mínima de 60 (sessenta) dias antes do seu término, estendendo-se até o limite máximo de 120 meses, nos termos do artigo 107, da Lei Federal 14.133/2021.

3.1.1. No caso de prorrogação será lavrado o Termo respectivo.

CLÁUSULA QUARTA – DAS RESPONSABILIDADES E OBRIGAÇÕES DA CONTRATADA

4.1. É de responsabilidade da Contratada executar o objeto do certame sob sua inteira responsabilidade, rigorosamente de acordo com as especificações contidas nos Anexos I e II. É salutar reafirmar que a Universidade USCS não aceitará fornecimento de equipamentos físicos e/ou virtuais ou ainda softwares e garantias, diferentes daqueles dispostos no termo de referência do edital 26/2025.

4.2. Manter durante a execução do contrato, em compatibilidade com as obrigações assumidas todas as condições de habilitação e qualificação exigidas no processo licitatório.

4.3. Responsabilizar pela pelo fornecimento dos bens e execução dos serviços objeto da licitação, cabendo ao seu representante na condição de preposto acompanhar o cumprimento rigoroso dos prazos, organização de reuniões, entrega de documentos, elaboração de relatórios de acompanhamento e quaisquer atividades pertinentes à execução dos serviços.

4.4. A Contratada deverá registrar as ocorrências havidas durante a execução do objeto dando ciência a Universidade Municipal de São Caetano do Sul, respondendo integralmente por sua omissão.

4.5. A Universidade USCS não assumirá nenhuma responsabilidade pelo pagamento de impostos e outros encargos que competirem à Contratada, nem se obrigará a fazer a essa qualquer restituição ou reembolso de quantias ou acessórios que a mesma despender com esses pagamentos.

4.6. A Contratada deverá prestar os serviços sempre por pessoal qualificado, respondendo perante a USCS e terceiros por todos os ônus, encargos, perdas e/ou danos porventura resultantes da execução do objeto da prestação de serviços.

4.7. A contratada deverá providenciar e custear pessoal habilitado em quantidade necessária para a execução dos serviços até o cumprimento integral do contrato.

4.8. A contratada deverá providenciar e custear os recursos computacionais (hardware software e/ou estrutura computacional em hosting) quando couber, utilizados por sua equipe de suporte técnico e de monitoramento NOC e de segurança de rede no desempenho de suas funções exigidas via celebração de contrato, respeitando-se as particularidades em cada lote contratado.

4.9. A Contratada deverá manter equipe de profissionais treinados nas melhores práticas e tecnologias existentes no mercado de cibersegurança.

4.10. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer dados, imagens produzidas ou informação de que tenha tomado ciência em razão da execução dos serviços discriminados neste instrumento, sem o consentimento, prévio e formal da Contratante.

4.11. A contratada poderá realizar subcontratação parcial do objeto (atividades relacionadas a etapa de fornecimento de equipamentos físicos e/ou virtuais e sua infraestrutura...), desde que tal subcontratação não diga respeito à atividade fim do objeto do certame, conforme disposto no artigo 122 da Lei 14.133/2021, contudo, sua efetiva realização deverá ser devidamente justificada e precedida expressamente de autorização da Universidade Municipal de São Caetano do Sul.

4.11.1. A subcontratação dos serviços será de inteira responsabilidade da contratada e deverá seguir as condições e especificações delimitadas para o objeto no termo de referência deste edital. Para efeito da respectiva subcontratação, a licitante apresentará à administração documentação que comprove capacitação técnica do subcontratado, que deverá ser avaliada e acostada aos autos do processo.

CLÁUSULA QUINTA - DO VALOR E DOS RECURSOS

5.1. Pelo fornecimento dos equipamentos firewall *as a service*, instalação, configuração, licenciamento e prestação de serviços de suporte técnico avançado de rede, manutenção e monitoramento NOC (24x7), elencados no lote 01, de acordo com as especificações e condições contidas nos anexos I e II deste instrumento contratual a Universidade USCS pagará à Contratada o valor global de R$ _____ (_____).

5.2. Pelo fornecimento da estrutura computacional em Data Center e Hosting, migração das palicações e bases de dados legado, instalação e configuração, além dos serviços de suporte técnico, manutenção e monitoramento NOC (24x7) descritos no lote 02, respeitando-se as especificações e condições contidas nos anexos I e II deste instrumento contratual a Universidade USCS pagará à Contratada o valor global de R$ _____ (_____).

5.3. As despesas onerarão a Classificação das despesas Orçamentárias, referenciada na dotação 12.364.1500.2.100.3.3.90.40.00, do orçamento da USCS, em conformidade com o disposto no parágrafo 1º do artigo 12 da Lei nº 10.320, de 16/12/1968.

CLÁUSULA SÉXTA – DO FATURAMENTO E DO PAGAMENTO

6.1. A Contratada quando do fornecimento dos equipamentos de firewall *as a service*, e/ou migração da base de dados legado, bem como execução dos serviços de instalação e configuração descritos nos respectivos lotes, deverá comunicar por escrito o evento e emitir a respectiva nota fiscal, encaminhando-a ao gestor/fiscalizador do contrato designado pela Universidade USCS para averiguação e emissão do respectivo termo de aceitação e liberação para posterior pagamento.

6.1.1. Os pagamentos serão efetuados à Contratada em parcela única, no prazo de até 10 (dez) dias úteis, contados do primeiro dia seguinte ao recebimento do Termo de Aceitação juntamente com a documentação fiscal completa (nota fiscal, fatura e demais documentos exigíveis), pelo setor de Contas a Pagar da Universidade USCS.

6.1.2. A emissão dos respectivos Termos de Aceitação, deverão ocorrer no prazo de até 05 dias, contados da comunicação formal da conclusão do fornecimento dos equipamentos e/ou dos serviços pela Contratada, devidamente atestados pelo gestor/fiscalizador do contrato.

6.2. Quanto ao Serviços descritos no anexo I referente aos lotes 01 e 02 (mensal).

6.2.1. **Faturamento mensal**

6.2.1.1. A(s) empresa(s) Contratada(s) emitirá(ão) nota fiscal mensal referente aos serviços de suporte técnico avançado 24x7, manutenção, monitoramento NOC, *(lote 01)* e/ou fornecimento de serviço de hospedagem computacional *in cloud*, serviço de suporte técnico 24x7, manutenção e monitoramento NOC (lote 02), no último dia útil do mês de prestação desses serviços, encaminhando-a ao gestor/fiscalizador do contrato, que deverá, no máximo no próximo dia útil efetuar a conferência, liberação e encaminhamento ao setor de contas a pagar da Universidade USCS.

6.2.1.2. O pagamento do serviço mensal será efetuado na 2ª(segunda) terça-feira do mês subsequente ao início dos serviços, desde que a nota fiscal e termo de liberação de pagamento emitido pelo gestor/fiscalizador do contrato seja encaminhado ao setor de contas a pagar da Contratante no prazo mencionado no subitem anterior.

6.2.1.2.1. Para efeito de pagamento no primeiro período (mês), considerando-se a aplicação do disposto no item 12.3 do instrumento convocatório, os serviços de suporte técnico 24x7, monitoramento NOC e segurança de rede 24x7, serão pagos de modo proporcional ao número de dias efetivos da prestação do serviço coberta pelo contrato nesse interim.

6.2.1.3. A ordem de pagamento será emitida pela seção de contas a pagar da USCS, a favor da Contratada, em agência do Banco _____, número _____ e conta corrente _____, ficando terminantemente vedada a negociação da duplicata mercantil na rede bancária ou com terceiros.

Parágrafo Primeiro**:** Caso o término da contagem aconteça em dias sem expediente bancário, o pagamento ocorrerá no primeiro dia útil imediatamente subsequente.

Parágrafo Segundo**:** Havendo divergência ou erro na emissão da documentação fiscal, será interrompida a contagem do prazo para fins de pagamento, sendo iniciada nova contagem somente após a regularização da documentação fiscal.

Parágrafo Terceiro**:** A constatação de irregularidades na execução deste ajuste motivará o desconto da importância correspondente ao descumprimento, sem prejuízo da eventual rescisão e aplicação das penalidades fixadas na cláusula décima.

6.3. A Universidade Municipal de São Caetano do Sul, poderá exigir a comprovação de quitação das obrigações trabalhistas vencidas relativas ao contrato, de acordo com disposto no § 3º do artigo 121 da Lei 14.133/2021 como condição para liberação de pagamento.

6.4. Eventualmente, em caso de atraso pela USCS no pagamento pelos serviços executados, desde que a empresa contratada não tenha concorrido de alguma forma para tanto, o valor devido deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para opagamento até a data do efetivo pagamento, à taxa de 6% (seis por cento) ao ano, aplicando-se a seguinte fórmula:

EM = I x N x VP

EM = Encargos Moratórios a serem acrescidos ao valor originalmente devido
I = Índice de atualização financeira, calculado segundo a fórmula:

I = (6 / 100) / 365

N = Número de dias entre a data limite prevista para o pagamento e a data do efetivo pagamento
VP = Valor atualizado da parcela em atraso de atraso

6.4.1. Em caso de atraso superior a 30 dias do vencimento, o valor principal será atualizado monetariamente pelo indicador de preços IPCA do último mês, anterior à data limite, divulgado pelo Instituto Brasileiro de Geografia e Estatística.

6.4.1.1. Para efeito de aplicação dos itens imediatamente acima, a empresa contratada deverá apresentar solicitação expressa e formal, ocasião em que se realizará a análise e negociação com a Universidade USCS.

CLÁUSULA SÉTIMA - DO REAJUSTE DE PREÇOS

7.1. Os valores constantes da proposta e expressos em reais para prestação dos serviços de suporte técnico, manutenção, monitoramento NOC (24x7), serviço de segurança firewall *as a service* (tipo 1, 2 e 3) referentes ao lote 01, bem como serviço de hospedagem da infraestrutura computacional em data center e hosting, serviço de suporte técnico, manutenção e monitoramento NOC (24x7) vinculados ao lote 02, descritos no anexo I deste instrumento de contrato, poderão sofrer reajustes somente após o interregno de 12 meses, contados a partir do prazo inscrito no subitem 2.1.5.2. deste instrumento contratual.

7.2. Na hipótese de manutenção do contrato, transcorridos os primeiros 12 meses, conforme expresso no subitem 7.1., o valor mensal decorrente dos serviços descritos no anexo I deste documento para os respectivos lotes, poderão ser reajustados partir do 13º (décimo terceiro) mês, de acordo com a variação do Índice Nacional de Preços ao Consumidor Amplo – IPCA/IBGE, em conformidade com a legislação em vigor ou por outro índice que venha substituí-lo.

7.3. O reajuste poderá ser concedido mediante expressa solicitação da Contratada, para análise e negociação com a USCS, e terá incidência de pagamento respeitando-se as condições e períodos estabelecidos no item 7.1.

CLÁUSULA OITAVA - DAS PENALIDADES

8.1. Comete infração administrativa, nos termos da Lei 14.133/2021, a proponente vencedora do certame e/ou contratada que der causa à inexecução parcial ou total do contrato; ensejar o retardamento da execução do instrumento; apresentar documentação ou praticar ato fraudulento durante a execução do

contrato; comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; praticar ato lesivo previsto no artigo 5º da Lei Federal 12.846/2013.

8.1.1. As empresas que cometerem as infrações dispostas no item 8.1, estarão sujeitas a aplicação de advertência, impedimento de licitar e contratar com a administração pública, ser declarada inidônea para licitar e contratar, além da aplicação de multas reparatórias e/ou moratórias, conforme o caso.

8.1.2. A aplicação das sanções previstas neste instrumento contratual não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Universidade USCS, bem como não impede essa administração de se utilizar cumulativamente da aplicação das sanções com as multas previstas.

8.2. A recusa injustificada da adjudicatária em aceitar ou retirar o termo de contrato, no prazo e nas condições estabelecidas caracterizará descumprimento total da obrigação assumida, sujeitando-o a juízo da Administração, nos termos da legislação, inclusive, municipal:

8.2.1. Ao pagamento de multa de 30% (trinta por cento) sobre o valor do contrato;

8.2.2. Ao pagamento correspondente à diferença de preço decorrente de nova licitação ou contratação, para o mesmo fim.

8.3. Pela inexecução total do contrato, será aplicada à Contratada a multa de 30% (trinta por cento) sobre o valor total do ajuste;

8.4. Pela inexecução parcial do contrato, será aplicada à Contratada a multa de 20% (vinte por cento) sobre o valor da obrigação não cumprida.

8.5. Pelo atraso injustificado a Contratada incorrerá em multa diária de 0,5% (cinco décimos por cento) sobre o valor do contrato, excluída, quando for o caso, a parcela correspondente aos impostos incidentes, quando destacados no documento fiscal, sendo que a aplicação da multa terá início no primeiro dia seguinte ao término do prazo contratual ou de execução do serviço.

8.5.1. Os atrasos injustificados superiores a 30 (trinta) dias corridos serão obrigatoriamente considerados inexecução total ou parcial, estando a Contratada sujeita as sanções previstas nos subitens 8.3 ou 8.4.

8.6. Além das multas e das penalidades aqui contidas, poderão ser aplicadas à Contratada, sanções decorrentes do não cumprimento das condições estabelecidas pelo ***Service Level Agreement*** que integra o Termo de Referência do edital, itens 1.14 e 2.13, conforme verificação e enquadramento do Gestor do instrumento de contrato designado pela USCS

8.7. As multas a que aludem os subitens anteriores não impedem que a Administração rescinda unilateralmente o contrato e aplique outras sanções previstas nas Leis Federais e Municipais, a saber:

8.7.1. Advertência, por escrito, no caso de pequenas irregularidades.

8.7.1.1. A sanção de advertência poderá ser aplicada nos seguintes casos:

I. Descumprimento das determinações necessárias à regularização das faltas ou defeitos observados na prestação dos serviços;

II. Outras ocorrências que possam acarretar transtornos no desenvolvimento dos serviços da Contratante, desde que não caiba a aplicação de sanção mais grave.

8.7.2. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração, pelo prazo de até dois anos, quando da inexecução contratual sobrevier prejuízo para a Administração;

8.7.2.1. A penalidade de suspensão será cabível quando a Contratada participar do certame e for verificada a existência de fatos que o impeçam de contratar com a Administração Pública. Caberá ainda a suspensão quando a Contratada, por descumprimento de cláusula contratual tenha causado transtornos no desenvolvimento dos serviços da Contratante.

8.7.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação.

8.7.3.1. Se a Contratada deixar de entregar a documentação ou apresentá-la falsamente, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará, pelo prazo de até cinco anos, impedido de contratar com a Administração Pública, sem prejuízo das multas previstas neste contrato e das demais cominações legais.

8.7.4. Verificado que a obrigação foi cumprida com atraso injustificado caracterizando a inexecução parcial, a Universidade Municipal de São Caetano do Sul poderá reter preventivamente, o valor da multa dos eventuais créditos que a Contratada tenha direito, até a decisão definitiva, assegurada a ampla defesa.

8.7.4.1. Se a USCS decidir pela não aplicação da multa, o valor retido será devolvido à Contratada.

8.8. Os atos previstos como infrações administrativas na Lei Federal nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.9. Independentemente das sanções retro, a Contratada ficará sujeita ainda, à composição das perdas e danos causados à Administração e decorrentes de sua inadimplência, bem como arcará com a correspondente diferença de preços verificada em nova contratação, na hipótese de os demais classificados não aceitarem a contratação pelos mesmos preços e prazos fixados pelo inadimplente.

8.10. A personalidade jurídica da empresa vencedora poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos no Edital ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a empresa vencedora.

8.11. É assegurada nos termos legais, os prazos para exercício do direito da ampla defesa e do contraditório, na aplicação das sanções previstas no escopo dos artigos 155 a 162 da Lei 14.133/2021, conforme o caso.

CLÁUSULA NONA - DA RESCISÃO

9.1. A falta de cumprimento das obrigações assumidas no presente instrumento ou a incidência do comportamento descrito no artigo 137 da Lei nº 14.133/2021, dará direito à USCS de rescindir, unilateralmente este contrato, independentemente de interpelação judicial, sendo aplicáveis, ainda, as disposições contidas no artigo 139 da mesma legislação. A rescisão contratual dar-se-á ainda em decorrência da aplicação dos termos contidos no artigo 138 da NLLC.

Parágrafo único

Quando da finalização ou eventualmente em caso de rescisão, a empresa detentora do instrumento contratual para fornecimento dos serviços descritos no termo de referência do edital concernentes ao **lote 02**, deverá disponibilizar à contratante o histórico das aplicações e bases de dados legado e dos dos serviços produzidos e armazenados durante o período contratual, em formato solicitado pelo Departamento de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul, no prazo de até 15 dias corridos.

CLÁUSULA DÉCIMA - DA GARANTIA CONTRATUAL

10.1. A(s) contratada(s), em até 10(dez) dias úteis contados da assinatura do contrato, deverá fazer prova de recolhimento, a título de Garantia de Execução do Contrato, equivalente a 5% (cinco por cento) do valor total pactuado, com vencimento para 60 (sessenta) dias após a data da entrega final dos serviços, correspondente a data da última parcela a ser paga pela Universidade Municipal de São Caetano do Sul, cabendo à Contratada optar por quaisquer modalidades assecuratórias previstas no parágrafo 1º do artigo 96 da Lei Federal 14.133/2021.

10.2. A garantia quando prestada nas modalidades fiança bancária e seguro garantia, deverá prever a cobertura de indenizações decorrentes de responsabilização da **Tomadora** dos serviços por obrigações assumidas pela Contratada, inclusive às concernentes aos encargos trabalhistas, previdenciários, fiscais e comerciais, nos termos deste contrato.

10.3. Na hipótese de o contratado optar pela modalidade de garantia inscrita no inciso II do parágrafo 1º do artigo 96 (Lei 14.133/2021), o prazo para prestação de garantia será assegurado nos termos do § 3º do mesmo artigo da mesma Lei.

10.4. Na hipótese de evidenciar qualquer impropriedade ou incorporação, a Contratante exigirá sua regularização ou substituição no prazo de 5(cinco) dias úteis da data de intimação.

10.5. A falta de atendimento à convocação para regularização ou substituição da garantia na forma e prazo especificado no item 10.4 acima, sujeitará a Contratada às seguintes consequências:

10.5.1. Retenção dos pagamentos que lhe sejam devidos, para recomposição da garantia contratual, na modalidade caução em dinheiro; ou

10.5.2. Caracterização de inexecução contratual, ensejando a consequente aplicação de penalidade prevista na cláusula 8ª deste documento e, ainda, a rescisão do ajuste com fundamento nos incisos do artigo 155 da Lei Federal nº 14.133/2021.

10.6. Caberá a Contratante decidir motivadamente entre a retenção de pagamentos para recomposição da garantia contratual ou a caracterização da inexecução contratual.

10.7. A correção monetária da garantia prestada na forma de caução em dinheiro será calculada com base na variação do índice IPCA/IBGE e, no caso de utilização de cheque, a data inicial da correção será a do crédito bancário.

CLÁUSULA DÉCIMA PRIMEIRA - DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

11.1. O agente público designado para assumir a função de Gestor do instrumento contratual resultante deste processo licitatório será o responsável pela Diretoria de Tecnologia da Informação e Inovação, cujas atribuições lhes permitirá ainda estabelecer os fiscalizadores técnicos. Os designados serão responsáveis pelo acompanhamento e execução do termo contratual objeto do presente certame, procedendo, de acordo com suas competências, ao registro das ocorrências e adotando as providências necessárias ao fiel cumprimento do ajuste, bem como, responsabilizar-se-ão pela vigência com o consequente controle dos prazos de início e término contratual, eventual prorrogação, aditamentos e instauração de novo processo de licitação quando couber.

11.2. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa.

11.3. O gestor do contrato deverá coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da autorização de fornecimento/ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

11.4. O gestor deverá elaborar relatório final contendo informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades relativas à administração e execução contratual.

11.5. Os fiscais técnicos do contrato anotarão para efeito de histórico de gerenciamento, todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. Identificada quaisquer irregularidades, este emitirá notificação, indicando o prazo para correção em sua execução.

11.6. Os fiscais técnicos comunicarão ao gestor desse instrumento, em prazo não inferior a 60 (sessenta) dias do término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

11.7. O gestor tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido por comissão, ou, pelo departamento competente para tal, em conformidade ao disposto no artigo 158 da Lei 14.133/2021.

11.8. Não obstante ser a Contratada a única e exclusiva responsável, inclusive perante terceiros, pela execução do objeto do contrato, reserva-se à USCS o direito de, sem que de qualquer forma restrinja a plenitude da responsabilidade da Contratada, exercer a mais ampla fiscalização dos serviços.

CLÁUSULA DÉCIMA SEGUNDA – DO FORO

12.1. Fica eleito o Foro da Comarca de São Caetano do Sul, Estado de São Paulo, com expressa renúncia de qualquer outro, por mais privilegiado que seja, para toda e qualquer ação oriunda deste ajuste e que não possa ser resolvida de comum acordo entre as partes.

12.2. E, por estarem justas e contratadas, as partes assinam o presente contrato em 2(duas) vias de igual teor e forma, perante a presença de 2(duas) testemunhas.

São Caetano do Sul, ____ de _____ de 2026.

_____	_____
Universidade Municipal de São Caetano do Sul	Nome da empresa
Contratante	**Contratada**

Testemunhas

_____	_____
Nome	Nome
CPF 000.***.***-00	CPF 000.***.***-00

TERMO DE CONFIDENCIALIDADE E RESPONSABILIDADE DE PROTEÇÃO DE DADOS PESSOAIS

Pregão Eletrônico nº26/2025
Processo de Compras nº 848/2025

_____(responsável ou representante legal da empresa), inscrito no CPF sob o nº _____, abaixo firmado, vinculado nestes termos ao Contrato nº _____/2026, no qual figura como Contratada a empresa _____, inscrita no CNPJ sob o nº _____, assumo o compromisso de manter confidencialidade e sigilo sobre todas as informações técnicas, bem como a responsabilidade e proteção dos dados pessoais na conformidade do disposto na Lei nº 13.709/2018 e suas alterações, como também a eventuais regulamentações relacionadas à Contratante, Universidade Municipal de São Caetano do Sul - USCS.

Comprometendo-me ainda, por este termo de confidencialidade e sigilo a não repassar o conhecimento das informações, responsabilizando-me pelos funcionários que vierem ter acesso às informações, obrigando a Contratada ao ressarcimento de quaisquer danos e/ou prejuízos oriundos de uma eventual quebra de sigilo ou confidencialidade das informações fornecidas.

Para os fins previstos neste termo e no Contrato, os termos a seguir serão interpretados conforme a legislação brasileira, notadamente Lei nº 13.709, de 14 de agosto de 2018 e alterações posteriores (a "Lei Geral de Proteção de Dados Pessoais" ou "LGPD"), com os seguintes significados:

- "**ANPD**" ou "**Autoridade Nacional de Proteção de Dados Pessoais**" é a autoridade regulatória máxima para dispor sobre assuntos de proteção de dados pessoais no Brasil.
- "Controladora" significa a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais, ou seja, nos moldes do presente Termo, a **USCS**.
- "**Dado Pessoal**" ou "**Dados Pessoais**" significa qualquer informação relacionada a pessoa natural identificada ou identificável, ou seja, que tenha o potencial de ser usada, de forma direta ou indireta, isoladamente ou em conjunto, para identificar uma pessoa natural.
- "**Dados Pessoais Sensíveis**" significa qualquer Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **"Legislação de Proteção de Dados"** significa qualquer legislação nacional, decretos, regulamentos, inclusive normas regulatórias emitidas pela ANPD, aplicável à proteção da privacidade e de Dados Pessoais no contexto do Tratamento de Dados Pessoais, incluindo, mas não se limitando à Lei Geral de Proteção de Dados Pessoais.
- **"Incidente de Segurança"** significa qualquer acesso não autorizado a Dados Pessoais e situações acidentais ou ilícitas de destruição, perda, alteração comunicação ou qualquer forma de Tratamento inadequado ou ilícito dos Dados Pessoais.
- **"Operadora"** significa a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome da Contratante e em conformidade com suas instruções legais, ou seja, nos termos do Contrato.
- **"Titular de Dados Pessoais"** ou "**Titular"** significa a pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.
- **"Tratamento"** significa toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, transferência, difusão ou extração de dados.

1. Das Informações Tecnológicas e Confidenciais

Não disponibilizar as informações tecnológicas e confidenciais, que em razão do desempenho da prestação dos serviços objeto do Contrato nº ____/2026 tiver acesso, tais como códigos fontes dos softwares de propriedade da USCS, Sistema de Gestão Acadêmica, bem como informações de propriedade da USCS que eventualmente sejam acessadas pela Contratada na consecução do objeto,

inclusive informações de clientes internos e externos. As demais informações confidenciais, incluindo, dentre outras, todas e quaisquer informações orais e/ou escritas, transmitidas e/ou divulgadas pela Contratante serão confidenciais, restritas e de propriedade desta.

Informações confidenciais e tecnológicas devem significar, sem se limitar, toda e qualquer informação, de natureza técnica, operacional, comercial, jurídica, know-how, planos de negócios, métodos de contabilidade, técnicas e experiências acumuladas, documentos, contratos, papéis, estudos, pareceres, pesquisas, códigos fontes, transmitida pela Contratante à Contratada.

2. Do Uso

A Contratada concorda em usar as informações confidenciais e tecnológicas recebidas da empresa como propósito restrito de se fazer cumprir o estabelecido no Contrato.

3. Da não Divulgação

A Contratada ao receber a informação confidencial somente poderá usá-la para o propósito estabelecido no item 2 acima e zelará para que tais informações confidenciais e tecnológicas não sejam de qualquer forma divulgadas ou reveladas a terceiros, utilizando-se, no mínimo, do mesmo zelo e cuidado que dispensa às suas próprias informações confidenciais.

4. Das Cópias

A Contratada fica desde já proibida de produzir cópias ou back-up sem licença da empresa, por qualquer meio ou forma, de quaisquer documentos fornecidos ou que tenham chegado ao seu conhecimento em virtude do Contrato, além daquelas imprescindíveis ao desenvolvimento de seu trabalho, considerando que todas sejam informações confidenciais.

5. Da Propriedade

Toda informação confidencial e tecnológica permanecerá sendo de propriedade da parte que revelar a informação confidencial, somente podendo ser usada pela parte receptora para os fins de execução do Contrato. Tais informações confidenciais e tecnológicas, incluídas as cópias realizadas serão retomadas à parte reveladora ou então destruídas pela parte receptora, tão logo que tenha terminado o prazo do Contrato.

6. Da Proteção de Dados Pessoais

Cada Parte se compromete a cumprir com o disposto na Legislação de Proteção de Dados na execução do objeto do Contrato. A Contratada poderá realizar o Tratamento de todos os Dados Pessoais em nome da Contratante nos termos do contrato limitando o acesso aos Dados Pessoais que tratar em nome da Contratante a seus colaboradores que tenham necessidade de acesso a tais Dados Pessoais para executarem as suas funções, assegurando que tais colaboradores sejam treinados com relação às obrigações de confidencialidade previstas nesse Termo e no Contrato, e concordem em cumpri-las.

6.1. A Contratada tratará os Dados Pessoais com a finalidade exclusiva e estritamente necessária ao cumprimento do Contrato e de acordo com as instruções legais da Contratante. A Contratada não irá realizar o Tratamento de Dados Pessoais para qualquer outra finalidade não prevista no Contrato, a menos que seja autorizada previamente por escrito pelo(s) representante(s) legal(is) da Contratante.

6.2. A Contratada não poderá transferir quaisquer Dados Pessoais relacionados ao Contrato, inclusive no que concerne ao armazenamento de dados em nuvem, salvo se previamente autorizado, por escrito, pela Contratante.

6.3. Dentro do prazo de 15 (quinze) dias (a) após os Dados Pessoais não mais serem necessários para os propósitos do Contrato, ou (b) após o encerramento do prazo do Contrato, ou, ainda, (c) por qualquer razão, como a devolução ou migração dos Dados Pessoais a outra empresa, por decisão da Contratante, a Contratada deverá após, destruir todos os Dados Pessoais em sua posse ou controle em decorrência do Contrato. Não obstante o disposto acima, a Contratada poderá manter uma cópia dos Dados Pessoais necessários ao cumprimento do prazo previsto na legislação aplicável, devendo a Contratada, nesse caso, informar para a Contratante quais Dados Pessoais serão mantidos, o prazo de sua guarda e qual o fundamento legal que justifica essa retenção. Após o término do prazo legal, a Contratada deverá destruir imediatamente os referidos Dados Pessoais. Nessa hipótese, as obrigações relativas a Dados Pessoais previstas neste instrumento continuarão em vigor até que todos os referidos Dados Pessoais sejam destruídos.

6.4. Não obstante quaisquer obrigações previstas no Contrato estabelecendo padrões para sistemas, aplicações, arquivos de dados e outras ferramentas de tecnologia, a Contratada garante que adotou e implementou, e manterá durante o prazo do Contrato, as medidas organizacionais e técnicas de segurança para proteger os Dados Pessoais contra destruição indevida, compartilhamento irregular ou

não-autorizado, perda acidental, alteração, acesso ou divulgação irregulares e/ou qualquer forma de Tratamento inadequado ou ilícito dos Dados Pessoais. A adequabilidade dessas medidas será avaliada à luz das técnicas mais modernas, custo de implementação, natureza dos Dados Pessoais e risco aos quais os Dados Pessoais estejam expostos. Essas medidas serão pelo menos iguais ou superiores a, cumulativamente: (i) qualquer regulamentação definida pela ANPD ou outro órgão governamental competente; (ii) padrões do ramo da Contratante e (iii) medidas que a Contratada adotar para proteger outro Dado Pessoal em sua posse ou controle.

6.5. Imediatamente e nunca em prazo superior a 24 (vinte e quatro) horas após tomar ciência ou suspeitar razoavelmente de qualquer Incidente de Segurança que possa comprometer a integridade, confidencialidade e/ou disponibilidade de qualquer Dado Pessoal, a Contratada deverá notificar a Contratante, por escrito, sobre tal fato. Referida notificação deverá, no mínimo:

(a) descrever a natureza dos Dados Pessoais afetados, as categorias e o número de titulares dos Dados Pessoais em questão;

(b) fornecer informações sobre os titulares de Dados Pessoais envolvidos;

(c) informar as medidas técnicas e de segurança utilizadas para a proteção dos Dados Pessoais;

(d) comunicar o nome e os detalhes de contato do encarregado ou responsável por proteção de Dados Pessoais da Contratada;

(e) descrever as prováveis consequências e riscos relacionados ao Incidente de Segurança;

(f) descrever as medidas adotadas ou propostas a serem adotadas para solucionar o Incidente Segurança; e

(g) descrever as medidas que foram ou serão tomadas para reverter ou mitigar os efeitos das perdas relacionadas ao Incidente de Segurança.

6.6. A Contratada deverá cooperar com a Contratante e adotar as medidas razoáveis, conforme as instruções da Contratante para auxiliar na investigação, mitigação e correção de cada Incidente de Segurança, permitindo à Contratante (i) realizar uma investigação completa sobre o Incidente de Segurança, (ii) formular uma resposta correta e adotar medidas adicionais adequadas em relação ao Incidente de Segurança, a fim de atender a qualquer requisito da legislação aplicável.

6.7. As Partes concordam em coordenar e cooperar de boa-fé no desenvolvimento do conteúdo de quaisquer declarações públicas relacionadas ou de quaisquer avisos necessários para os Titulares afetados pelo Incidente de Segurança ou para a ANPD. A Contratada não deve informar terceiros sem antes obter o consentimento prévio, por escrito, da Contratante, a menos que seja exigida notificação pela legislação à qual a Contratada esteja sujeita. Nesse caso, a Contratada deverá, na máxima extensão permitida pela legislação aplicável, informar a Contratante sobre tal requisito legal, fornecer uma cópia da(s) notificação(ões) proposta(s) e considerar os comentários feitos pela Contratante, antes de notificar a quaisquer terceiros sobre o Incidente de Segurança.

> **6.7.1.** Se a Contratante incorrer em custos, diretos ou indiretos, em razão do Incidente de Segurança, incluindo investigar, remediar e mitigar o seu impacto, a Contratada concorda em reembolsar a Contratante dos respectivos custos. Mediante correção satisfatória do Incidente de Segurança, a Contratada concorda em tomar ações razoavelmente necessárias para evitar nova ocorrência e fornecerá declarações escritas para a Contratante sobre as medidas apropriadas que foram tomadas para proteger a Contratada contra a ameaça de uma ocorrência de fato similar.

6.8. A contratada notificará a contratante, imediatamente, sobre qualquer solicitação recebida de um titular cujos dados pessoais estejam sendo tratados pela contratada em razão do contrato. A contratada concorda em cumprir com todas as instruções razoáveis solicitadas pela contratante quanto à resposta a tal solicitação individual e a não responder a qualquer solicitação de titular de dados pessoais diretamente. Além disso, a contratada concorda em fornecer toda e qualquer assistência requerida pela contratante para responder, dentro do período exigido pela legislação de proteção de dados ou política da contratante, a qualquer solicitação individual recebida pela contratada ou pela contratante.

6.9. A Contratada concorda em responder total e em até 2 (dois) dias úteis a todos os questionamentos da Contratante relacionados ao Tratamento de Dados Pessoais relativos ao Contrato, e auxiliar a Contratante a responder total e prontamente aos questionamentos de qualquer autoridade competente relativos ao Tratamento de Dados Pessoais relacionado ao Contrato, incluindo a ANPD. A Contratada notificará a Contratante imediatamente de qualquer solicitação efetuada pela ANPD ou outra autoridade competente para divulgar Dados Pessoais que a Contratada trate em nome da Contratante, salvo se tal comunicação for proibida pela Legislação. Adicionalmente, a Contratada concorda em cooperar com a Contratante para responder ou objetar tal solicitação.

6.10. A Contratada concorda que, mediante requisição razoável da Contratante, disponibilizará suas instalações para auditoria de conformidade da Contratante em relação às obrigações deste Termo ou do Contrato, a ser realizada pela própria Contratante ou empresa designada pela Contratante. A Contratada deverá cooperar integral e satisfatoriamente com a referida auditoria. No caso dessa auditoria revelar falhas materiais ou fragilidades nos esforços de proteção de Dados Pessoais por parte da Contratada, a Contratante terá o direito de suspender ou terminar o Contrato, bem como a execução dos serviços que

acarretam o Tratamento de Dados Pessoais até que tais medidas sejam resolvidas adequadamente.

6.11. A Contratada defenderá, indenizará e manterá indene a Contratante de quaisquer demandas, exigências, despesas, danos, perdas, custos, taxas ou penalidades decorrentes do descumprimento da Contratada da Legislação de Proteção de Dados, bem como do Contrato. Não obstante qualquer previsão no Contrato em contrário, as obrigações de indenização estabelecidas neste item não estarão sujeitas a nenhuma limitação de responsabilidade da Contratada.

6.12. A Contratada declara e garante que:

(a) realizará Tratamento dos Dados Pessoais tão somente dentro dos limites e na medida em que for autorizado pela Contratada, conforme suas instruções explícitas;

(b) caso a Contratada perceba que será incapaz de cumprir com os requisitos exigidos pela Legislação de Proteção da Dados, comunicará tal fato imediatamente e por escrito à Contratante, que poderá, a seu único e exclusivo critério, suspender a transferência de Dados Pessoais ou rescindir o Contrato;

(c) irá realizar a criptografia de quaisquer Dados Pessoais Sensíveis armazenados em aparelhos portáteis, bem como de todo Dado Pessoal solicitado pela Contratante, dentro do que lhe for razoavelmente exigido;

(d) não tem conhecimento de nenhum Incidente de Segurança nos últimos 5 (cinco) anos que possa afetar o Contrato ou a outra Parte; e

(e) encontra-se plenamente capaz de cumprir com os termos e condições do presente Termo, do Contrato e da Legislação de Proteção de Dados e que, no evento de uma relevante alteração das normas aplicáveis às atividades de Tratamento de Dados Pessoais que tenha potencial de modificar sua conformidade legal e contratual, notificará a Contratante imediatamente; e

(f) implementou todas as medidas organizacionais e técnicas de segurança exigidas nos termos do Contrato da Legislação de Proteção de Dados.

7. Da Responsabilidade

A Contratada se obriga a não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações confidenciais para nenhuma pessoa, física ou jurídica e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objeto referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o seu uso indevido por qualquer pessoa que, por qualquer razão tenha tido acesso a elas.

Restituir imediatamente o documento ou outro suporte que contiver informações sigilosas à parte reveladora, sempre que esta as solicitar ou sempre que as informações deixarem de ser necessárias e, não guardar para si, em nenhuma hipótese, cópia, reprodução ou segunda via das mesmas.

8. Da violação

A Contratada que recebe e tem conhecimento de informação confidencial, reconhece e aceita que, na hipótese de violação de quaisquer das cláusulas deste Termo, estará sujeito as sanções e penalidades legais conforme as Leis 9.609/1998 e 14.133/2021, sem prejuízo das perdas e danos que der causa, inclusive as de ordem moral ou concorrencial, bem como as de responsabilidades civis e criminais respectivas.

9. Do Prazo

A vigência da obrigação de confidencialidade, sigilo, proteção e responsabilidade pelos Dados Pessoais assumida pela minha pessoa por meio deste Termo e, por conseguinte a empresa denominada Contratada terá validade pelo tempo que perdurar o Contrato e disponibilização de informações por parte da Contratante.

São Caetano do Sul, ____ de _____de 2026.

_____

Nome e assinatura do responsável pelo contrato

Testemunhas

_____

Nome

CPF 000.***.***-00

_____

Nome

CPF 000.***.***-00

ANEXO I

Instrumento Contratual nº ____/2026
Processo de Compras nº848/2025

OBJETIVO

O presente documento, transcrito a partir do termo de referência do edital, teve como objetivo a contratação de empresa especializada para fornecimento de infraestrutura e serviços de hospedagem em nuvem, bem como solução de segurança perimetral (Next Generation Firewall) para atendimento ao ambiente de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul - USCS, conforme especificações e condições contidas no edital de número 26/2025.

1. <u>Especificações e Exigências Aplicadas ao Lote 01</u>

a. Unidades da Universidade Municipal de São Caetano do Sul a serem atendidos nesse projeto desses serviços:

No quadro imediatamente abaixo, há o detalhamento das unidades da Universidade de São Caetano do Sul que deverão realizar a contratação dos respectivos serviços destacados neste termo de referência.

DIMENSIONAMENTO	Universidade Municipal de São Caetano do Sul					
	UNIDADE BARCELONA Endereço: Av. Goiás, 3400 - Barcelona, São Caetano do Sul - SP, CEP: 09550-051.	UNIDADE CENTRO Endereço: R. Santo Antônio, 50 - Centro, São Caetano do Sul - SP, CEP: 09521-160.	UNIDADE CENTRO 2 Endereço: Rua Samuel Klein, 83 2° Andar - Centro - São Caetano do Sul - CEP: 09510-125.	UNIDADE CONCEIÇÃO Endereço: Rua Conceição, 321 - Santo Antônio - São Caetano do Sul - 09530-060.	UNIDADE ITAPETININGA Endereço: Av. Dr. Ciro Albuquerque, 4750 - Taboãozinho, Itapetininga - SP, CEP: 18200-021.	UNIDADE MANOEL COELHO Endereço: Rua Manoel Coelho, 600 - 6º andar - Centro, São Caetano do Sul - SP, Cep: 09510-101.
	Serviço tipo: 1.	**Serviço tipo: 1.**	**Serviço tipo: 3.**	**Serviço tipo: 2.**	**Serviço tipo: 3.**	**Serviço tipo: 3.**
	As unidades destacadas são as responsáveis por receber as instalações locais, garantindo que todo o processo de implementação e configuração seja realizado de forma adequada e eficiente. Essas unidades desempenham um papel fundamental na adaptação das soluções aos requisitos específicos de cada local, assegurando que os recursos necessários para o bom funcionamento das operações estejam corretamente instalados e configurados.					

b. No escopo dessa contratação, em particular o lote 01, essa administração tem a pretensão de contratar no mercado empresa com expertise para fornecer serviço de segurança de rede baseada em equipamento de firewall *as a service*, integrada a prestação de serviços de suporte técnico, manutenção e monitoramento no formato 24x7, por período de 24 meses. No quadro abaixo, relaciona-se os diversos serviços objeto de contratação e sua categorização.

A Contratada será responsável pela aquisição, entrega, implementação e configuração e licenciamento de todos os equipamentos *as a service* necessários e descritos no quadro a seguir desse documento, não sendo aceito a entrega de outros hardwares que não contemplem plenamente as especificações elencadas neste termo de referência.

LOTE 01	Item	Descrição	Quantidade em meses
		SERVIÇO DE SEGURANÇA FIREWALL *AS A SERVICE* TIPO **1**.	24
		SERVIÇO DE SEGURANÇA FIREWALL *AS A SERVICE* TIPO **2**.	24
		SERVIÇO DE SEGURANÇA FIREWALL *AS A SERVICE* TIPO **3**.	24
		SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	01
		SERVIÇO DE SUPORTE TÉCNICO COM ATENDIMENTO LOCAL E REMOTO	24
		SERVIÇO DE MONITORAMENTO (NOC)	24

1.1. SOLUÇÃO DE FIREWALL DE PROXIMA GERAÇÃO.

1.1.1. Deverá ser fornecida uma solução de firewall de próxima geração (NGFW – Next Generation Firewall) em alta disponibilidade, no modo ativo/ativo, ou seja, no mínimo dois equipamentos funcionando simultaneamente para todas as unidades da universidade.

1.1.2. Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos e efetuar os necessários ajustes sem ônus para o contratante desde que os danos causados não sejam decorrentes do mau uso, imperícia ou imprudência;

1.1.3. Os equipamentos devem ser iguais e suportar no mínimo as seguintes configurações e ser configuradas de acordo com ambiente:

1.1.4. Especificações Gerais:

1.1.4.1. Os equipamentos a serem utilizados deverá fornecer logs e relatórios embarcados, com armazenamento histórico mínimo de 120 dias, contendo no mínimo os itens abaixo:

- Dashboard com informações do sistema:
- Informações de CPU
- Informações do uso da rede.
- Informações de memória.

- Informações de atividades de navegação.
- Permitir visualizar número políticas ativas.
- Visualizar número de usuários conectados remotamente.
- Visualizar número de usuários conectados localmente.

1.1.5. Relatórios com informações sobre as conexões de origem e destino por países.
1.1.6. Relatórios informando as conexões dos hosts.
1.1.7. Visualizar relatórios por período, permitindo o agendamento e envio destes relatórios por e-mail.
1.1.8. Permitir exportar relatórios para as seguintes extensões/plataformas:

- PDF
- HTML
- Excel
- Permitir visualizar relatório de políticas ativas associado ao ID da política criada.
- Relatório que informe o uso IPSEC por host e usuário.
- Relatório que informe o uso L2TP por host e usuário.
- Relatório que informe o uso PPTP por usuários.
- Relatório abordando eventos de VPN.
- Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações:
- Logs do sistema;
- Logs das políticas de segurança;
- Logs de autenticação;
- Logs de administração do firewall NGFW.
- Permitir ocultar os relatórios usuários e IPs cadastrados.

➢ TIPIFICAÇÃO DA SOLUÇÃO DE FIREWALL QUE SERÁ CONTRATADA

1.1.9. **A SOLUÇÃO DO TIPO 1** deverá possuir no mínimo as seguintes configurações tanto quanto de software como de hardware:
1.1.9.1. Modalidade de configuração, alta disponibilidade e dois equipamentos configurados como ativo/ativo.
1.1.9.2. Possuir no mínimo 4 interfaces 10/100/1000 base-T;
1.1.9.3. Possuir no mínimo 4 interfaces 2,5GbE base-T;
1.1.9.4. Possuir no mínimo 4 interfaces SFP+ 10GbE;
1.1.9.5. Deve possuir no mínimo 2 portas que suportem by-pass;
1.1.9.6. Deve possuir no mínimo 2 portas que suportem by-pass;
1.1.9.7. A solução proposta deve corresponder aos seguintes critérios:

- Suportar no mínimo 368.000 novas conexões por segundo;
- Suportar no mínimo 16.600.000 conexões simultâneas;
- Possuir no mínimo 75 Gbps de rendimento (throughput) do Firewall;
- No mínimo 29.500 Mbps de rendimento (throughput) de IPS;
- Possuir no mínimo 3,2 (três inteiros e dois décimos) Gbps de throughput de VPN AES.
- Deverá possuir no mínimo 25.200 Mbps de taxa de transferência de Threat Protection.
- Latência do Firewall máxima (UDP de 64 bytes) 3 µs.
- IPsec VPN throughput deverá suportar no mínimo 62.500 Mbps.
- Quantidade mínima de túneis simultâneos VPN IPsec 8.500.
- Quantidade mínima de Túneis simultâneos SSL VPN 7.500.
- Inspeção SSL/TLS de 8.000 Mbps no mínimo.
- Deve possuir um interruptor de alimentação.
- Conexões SSL/ TLS simultâneas 276480.

1.1.10. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.1.11. A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
1.1.12. A solução proposta deve possuir no mínimo 240 GB de espaço em disco SSD SATA-III para o armazenamento local de eventos e relatórios.
1.1.13. Possuir pelo menos, 2 (dois) slots para adição de módulo de portas;
1.1.14. Deverá possuir Pinos de montagem para externo fonte de energia.
1.1.15. Ter o peso máximo após desembalado de 9 kg.
1.1.16. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
1.1.17. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
1.1.18. Deverá ter disponível pelo menos 2 conexões USB 3.0.
1.1.19. Não deverá possuir limitação na quantidade de VPN via Software.
1.1.20. Deverá possuir um display LCD, multifuncional e na parte frontal do firewall
1.1.21. Número irrestrito de usuários/IP conectados.
1.1.22. O equipamento deve ter no máximo 1 (um) U de altura para montagem em rack.

1.1.23. **A SOLUÇÃO DO TIPO 2** deverá possuir no mínimo as seguintes configurações tanto quanto de software como de hardware:

1.1.24. Modalidade de configuração, alta disponibilidade e dois equipamentos configurados como ativo/ativo.
1.1.25. Possuir no mínimo 8 interfaces 10/100/1000 base-T e 2 SFP 1GbE;
1.1.26. Possuir no mínimo 2 interfaces SFP+ 10GbE;
1.1.27. Deve possuir no mínimo 1 porta que suportem by-pass;
1.1.28. A solução proposta deve corresponder aos seguintes critérios:

- Suportar no mínimo 186.500 novas conexões por segundo;
- Suportar no mínimo 12.260.000 conexões simultâneas;
- Possuir no mínimo 47 Gbps de rendimento (throughput) do Firewall;
- No mínimo 10.500 Mbps de rendimento (throughput) de IPS;
- Deverá possuir no mínimo 7.400 Mbps de taxa de transferência do Threat Protection.
- Latência do Firewall máxima (UDP de 64 bytes) 4 µs.
- IPsec VPN throughput deverá suportar no mínimo 25.000 Mbps.
- Quantidade mínima de túneis simultâneos VPN IPsec 6.500.
- Quantidade mínima de Túneis simultâneos SSL VPN 5.000.
- Inspeção SSL/TLS de 2.470 Mbps no mínimo.
- Quantidade mínima de conexões simultâneas SSL/TLS de 55.290.
- Deve possuir um interruptor de alimentação.

1.1.29. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.1.30. A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
1.1.31. A solução proposta deve possuir no mínimo 240 GB de espaço em disco SSD SATA-III para o armazenamento local de eventos e relatórios.
1.1.32. Possuir slot para adição de módulo de portas;
1.1.33. Deverá possuir Pinos de montagem para externo fonte de energia.
1.1.34. Ter o peso máximo após desembalado de 5 kg.
1.1.35. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
1.1.36. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
1.1.37. Deverá ter disponível pelo menos 2 conexões USB 3.0 e 1 conexão 2.0
1.1.38. Não deverá possuir limitação na quantidade de VPN via Software.
1.1.39. Deverá possuir um display LCD, multifuncional e na parte frontal do firewall
1.1.40. Número irrestrito de usuários/IP conectados.
1.1.41. O equipamento deve ter no máximo 1 (um) U de altura para montagem em rack 19”.

1.1.42. **A SOLUÇÃO DO TIPO 3** deverá possuir no mínimo as seguintes configurações tanto quanto de software como de hardware:
1.1.43. Modalidade de configuração, alta disponibilidade e dois equipamentos configurados como ativo/ativo.
1.1.44. Possuir no mínimo 4 interfaces 10/100/1000 base-T;
1.1.45. Possuir no mínimo 2 interfaces 2,5 GbE base-T PoE de no mínimo 30w;
1.1.46. Possuir no mínimo 2 interfaces SFP+ 10GE fiber;
1.1.47. A solução proposta deve corresponder aos seguintes critérios:

- Suportar no mínimo 105.000 novas conexões por segundo;
- Suportar no mínimo 6.400.000 conexões simultâneas;
- Possuir no mínimo 19,1 Gbps de rendimento (throughput) do Firewall;
- No mínimo 5.800 Mbps de rendimento (throughput) de IPS;
- Deverá possuir no mínimo 4.750 Mbps de taxa de transferência do Threat Protection.
- IPsec VPN throughput deverá suportar no mínimo 6.350 Mbps.
- Quantidade mínima de túneis simultâneos VPN IPsec 2.500.
- Quantidade mínima de Túneis simultâneos SSL VPN 1.500.
- Inspeção SSL/TLS de 1.700 Mbps no mínimo.
- Quantidade mínima de conexões simultâneas SSL/TLS de 18.432.
- Deve possuir um interruptor de alimentação.

1.1.48. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.1.49. A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
1.1.50. A solução proposta deve possuir no mínimo 64 GB de espaço para o armazenamento local de eventos e relatórios.
1.1.51. Possuir slot para adição de módulo de portas;
1.1.52. Ter o peso máximo após desembalado de 3 kg.
1.1.53. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
1.1.54. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
1.1.55. Deverá ter disponível pelo menos 1 conexão USB 3.0 e 1 conexão 2.0
1.1.56. Não deverá possuir limitação na quantidade de VPN via Software.
1.1.57. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e console.

1.1.58. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup) das configurações, incluindo os objetos de usuário.
1.1.59. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.
1.1.60. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.
1.1.61. A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário.
1.1.62. A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory.
1.1.63. Suporte à autenticação do Chromebook.
1.1.64. Os tipos de autenticação devem ser, modo transparente, por autenticação NTLM e cliente de autenticação nas máquinas.
1.1.65. Fornecer clientes de autenticação para Windows, MacOS X, Linux 32/64.
1.1.66. Certificados de autenticação para iOS e Android.
1.1.67. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.
1.1.68. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.
1.1.69. A solução proposta deve suportar NTP.
1.1.70. A solução proposta deverá suportar a funcionalidade de unir usuário/IP/MAC para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.
1.1.71. A solução proposta deve ter suporte multilíngue para console de administração web.
1.1.72. A solução proposta deverá suportar fazer um rollback de versão.
1.1.73. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.
1.1.74. A solução proposta deve suportar instalação de LAN by-pass no caso do firewall NGFW estar configurado no modo transparente.
1.1.75. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que o PPPoE mudar.
1.1.76. A solução proposta deve suportar SNMP v1, v2c.
1.1.77. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.
1.1.78. A solução proposta deve ser baseada em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança.
1.1.79. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.
1.1.80. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação).
1.1.81. A solução proposta deve atender terminais (Microsoft) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.
1.1.82. A solução proposta deve suportar:
1.1.83. Serviço de DHCP/DHCPv6;
1.1.84. Serviço de DHCP/DHCPv6 Relay Agent;
1.1.85. A solução proposta deve trabalhar como DNS/DNSv6 Proxy.
1.1.86. Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting.
1.1.87. Permitir exportar informações de troubleshooting para arquivo PCAP.
1.1.88. Reutilização de definições de objetos de rede, hosts, serviços, período, usuários, grupos, clientes e servers.
1.1.89. Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades específicas a ele.
1.1.90. Controle de acesso e dispositivos por zoneamento.
1.1.91. Integrar com ferramenta de gerenciamento centralizado disponibilizado pelo próprio fabricante.
1.1.92. Traps SNMP ou e-mail para notificações do sistema.
1.1.93. Suportar envio de informações via Netflow e possuir informações via SNMP.

1.2. BALANCEAMENTO DE CARGA E REDUNDÂNCIA PARA MÚLTIPLOS PROVEDORES DE INTERNET

1.2.1. A solução proposta deve suportar o balanceamento de carga e redundância (Failover) para no mínimo 2 (dois) links de Internet.
1.2.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.
1.2.3. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga.
1.2.4. A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP.
1.2.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.
1.2.6. A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin".
1.2.7. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet, bem como tráfego IPv4 e IPv6.

1.3. ALTA DISPONIBILIDADE

1.3.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) no modelo ativo/ativo.
1.3.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways, mantendo a Alta Disponibilidade.
1.3.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.
1.3.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.

1.3.5. A solução proposta deve suportar sincronização automática e manual entre os firewalls NGFWs em "cluster".
1.3.6. A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge).

1.4. ESPECIFICAÇÕES DO FIREWALL E ROTEAMENTO

1.4.1. A solução deve ser Standalone Firewall NGFW e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança.
1.4.2. A solução proposta deve suportar “Stateful Inspection” baseado no usuário "one-to-one", NAT Dinâmico e PAT.
1.4.3. A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall.
1.4.4. A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga, baseado na mesma regra do Firewall para facilitar de uso.
1.4.5. A solução proposta deve suportar arquitetura de segurança baseado em Zonas.
1.4.6. A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".
1.4.7. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.
1.4.8. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).
1.4.9. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.
1.4.10. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.
1.4.11. O sistema proposto deve prover mensagem de alertas no Dashboard (Painel de Bordo) quando eventos como, por exemplo: nova firmware disponível para download ou a licença irá expirar em breve.
1.4.12. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address).
1.4.13. A solução proposta deve suportar IPv6.
1.4.14. A solução proposta deve suportar implementações de IPv6 Dual Stack.
1.4.15. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd.
1.4.16. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.
1.4.17. A solução proposta deve suportar DNSv6.
1.4.18. A solução proposta deve oferecer proteção DoS contra ataques IPv6.
1.4.19. A solução proposta deve oferecer prevenção contra Spoof em IPv6.
1.4.20. A solução proposta deve suportar 802.3ad para Link Aggregation.
1.4.21. A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga.
1.4.22. A solução proposta deve suportar gerenciamento de banda baseado em aplicação, que permite administradores criarem políticas de banda de utilização de link baseado por aplicação.
1.4.23. Flood protection, DoS, DDoS e Portscan.
1.4.24. Bloqueio de Países baseados em GeoIP.
1.4.25. Suporte a Upstream proxy.
1.4.26. Suporte a VLAN DHCP e tagging.
1.4.27. Suporte a Multiple bridge.
1.4.28. Funcionalidades do portal do usuário.
1.4.29. Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).
1.4.30. Download dos clientes de autenticação disponibilizados pela ferramenta.
1.4.31. Download do cliente VPN SSL em plataformas Windows.
1.4.32. Download das configurações SSL em outras plataformas.
1.4.33. Informações de hotspot.
1.4.34. Autonomia de troca de senha do usuário.
1.4.35. Visualização do uso de internet do usuário conectado.
1.4.36. Acesso a mensagens em quarentena.
1.4.37. Opções base de VPN.
1.4.38. Site-to-site VPN: SSL, IPSec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key.
1.4.39. L2TP e PPTP.
1.4.40. VPN SSL, IPSEC.
1.4.41. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

1.5. FUNCIONALIDADES BASE DE QOS E QUOTAS

1.5.1. QoS aplicado a redes e usuários de download/upload em tráfegos baseados em serviços.
1.5.2. Otimização em tempo real do protocolo VoIP.
1.5.3. Suporte a marcação DSCP.
1.5.4. Regras associadas por usuário.
1.5.5. Criar regras que limitem e garantam upload e download.
1.5.6. Permitir criar regra de QoS individualmente e compartilhada.

1.6. FILTRAGEM E SEGURANÇA WEB

1.6.1. Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web.
1.6.2. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas, agregadas a pelo menos 75 categorias oferecidas pela solução.

1.6.3. Realizar autenticação dos usuários nos modos transparente e padrão.
1.6.4. As autenticações devem ser feitas via NTLM.
1.6.5. Possuir sistema de quotas aplicado por usuários e grupos.
1.6.6. Permitir criar políticas por horário aplicado a usuários e grupos.
1.6.7. Possuir sistema de malware scanning que realize as seguintes ações:

- Bloquear toda forma de vírus
- Bloquear malwares web
- Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acesso web (via navegador).

1.6.8. Prover proteção em tempo real de todos os acessos web.
1.6.9. A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças.
1.6.10. Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.
1.6.11. Fornecer Pharming Protection.
1.6.12. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.
1.6.13. Permitir criação de regras customizadas baseadas em usuário e hosts.
1.6.14. Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy.
1.6.15. Validação de certificado.
1.6.16. Prover cache de navegação, contribuindo na agilidade dos acessos à internet.
1.6.17. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)
1.6.18. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.
1.6.19. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.
1.6.20. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.
1.6.21. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.
1.6.22. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.
1.6.23. Range aceitável de 1 a 25600KB.
1.6.24. Bloquear tráfego que não segue os padrões do protocolo HTTP.
1.6.25. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.
1.6.26. Nas exceções, permitir definir operadores “AND” e “OR”.
1.6.27. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.
1.6.28. Permitir definir nas exceções a opção de não realizar escaneamento contra malware.
1.6.29. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.
1.6.30. Permitir criar regras de exceções por endereços IPs de origem.
1.6.31. Permitir criar regras de exceções por endereços IPs de destino.
1.6.32. Permitir criar exceções por grupo de usuários.
1.6.33. Permitir criar exceções por categorias de sites.
1.6.34. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.
1.6.35. Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: “Criminal Activities, Finance & Investing, Games and Gambling”, entre outras.
1.6.36. Permitir editar grupos de categorias pré-estabelecidos pela solução.
1.6.37. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações:

- Nome da regra;
- Permitir criar uma descrição para identificação da regra.
- Ter a possibilidade de classificação de pelo menos: Produtivo ou Não produtivo;
- Permitir aplicar Traffic shaping diretamente na categoria.
- Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave.
- Deve permitir importar uma base com domínios e palavras-chaves na hora da criação da categoria, a base com informações de domínios e palavras-chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt.
- Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro.

1.6.38. Ter função para criar grupos de URLs.
1.6.39. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.
1.6.40. Permitir ao administrador especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.
1.6.41. Deve permitir que em uma mesma política sejam aplicadas ações diferentes de acordo com o usuário autenticado.
1.6.42. Nas configurações das políticas deve-se existir pelo menos as opções de: Liberar categoria/URL, bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.
1.6.43. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.
1.6.44. Permitir criar cotas de navegação com os seguintes requisitos:
1.6.45. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.

1.7. CONTROLE E SEGURANÇA DE APLICAÇÕES

1.7.1. Prover controle para mais de 2500 aplicações diferentes.

1.7.2. Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.
1.7.3. Permitir criar regras de controle por usuário e hosts.
1.7.4. Permitir realizar traffic shaping por aplicação e grupo de aplicações.
1.7.5. Possibilitar que as regras criadas baseadas em aplicação permitam:
- Bloquear o tráfego para as aplicações
- Liberar o tráfego para as aplicações
- Criar categorização das aplicações por risco:
- Risco muito baixo
- Risco baixo
- Risco médio
- Risco alto
- Risco muito alto

1.7.6. Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.
1.7.7. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.
1.7.8. Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao youtube, mas bloquear o upload de vídeos, e etc.
1.7.9. Permitir agendar um horário e data específica para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

1.8. PROTEÇÃO DE REDE

1.8.1. Prover funcionalidade de Intrusion Prevention System (IPS).
1.8.2. Proporcionar alta performance na inspeção dos pacotes.
1.8.3. Possuir mais de 6500 assinaturas conhecidas.
1.8.4. Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.
1.8.5. Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.
1.8.6. Possuir funcionalidade Anti-DoS.
1.8.7. Deve-se permitir customizar os valores das seguintes funcionalidades de DoS:
- SYN Flood
- UDP Flood
- TCP Flood
- ICMP Flood
- IP Flood

1.8.8. Possuir templates pré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ e etc.
1.8.9. Possuir proteção contra spoofing.
1.8.10. Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.
1.8.11. Possuir funcionalidade para o administrador poder criar by-pass de DoS.
1.8.12. Permitir ao administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.

1.9. PROTEÇÃO AVANÇADA CONTRA AMEAÇAS PERSISTENTES (APT)

1.9.1. Detectar e bloquear tráfego de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.
1.9.2. Possuir logs e relatórios que informem todos os eventos de APT.
1.9.3. Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.
1.9.4. Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.
1.9.5. Proteção para E-mails
1.9.6. Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.
1.9.7. Possuir serviço de reputação para monitoramento dos fluxos dos e-mails, sendo assim, o AntiSpam deverá bloquear e-mails considerados com má reputação na internet e pelo fabricante.
1.9.8. Bloquear SPAN e MALWARES durante a transação SMTP.
1.9.9. Possuir duas engines de antivírus para duplo escaneamento.
1.9.10. Ter proteção em tempo real, sendo que a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos e-mails que passam pela solução e assim tomar ações automáticas de segurança, caso necessário.
1.9.11. Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.
1.9.12. Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.
1.9.13. Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customizá-los de acordo com o desejado.
1.9.14. Ter suporte a criptografia TLS para SMTP, POP e IMAP.
1.9.15. As ações dos e-mails considerados SPAM devem ser:
- Drop
- Warn
- Quarantine

1.9.16. Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: SPAM Marketing etc. etc. etc.
1.9.17. Permitir visualizar os e-mails que se encontram na fila para serem enviadas.
1.9.18. Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.
1.9.19. Possuir funcionalidade de allowlist e blocklist.
1.9.20. Possuir funcionalidade que rejeite e-mails com HELO inválido e/ou que não possuam RDNS.
1.9.21. Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.
1.9.22. Prover ambiente de Sandbox na nuvem provido pelo próprio fabricante.
1.9.23. Realizar inspeções de executáveis e documentos que possuam conteúdo executáveis.
1.9.24. Possuir suporte aos principais executáveis Windows como: .exe, .com e .dll
1.9.25. Possuir suporte aos principais documentos do Word como: .doc, .docx, .docm e .rft.
1.9.26. Realizar análise em documentos PDF.
1.9.27. Realizar análise de qualquer tipo de conteúdo que possua os seguintes tipos de arquivos: ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet.
1.9.28. Suporte a mais de 20 tipos de arquivos e extensões.
1.9.29. Realizar análises dinâmicas de malwares e ameaças, rodando estes arquivos em ambientes reais e em produção, todos providos na nuvem pelo fabricante.
1.9.30. Relatórios detalhados das ameaças bem como visibilidade dos alertas na dashboard da solução.
1.9.31. O tempo em média das análises devem ser menores do que 120 segundos.
1.9.32. Suportar a análise de links de download em tempo real.
1.9.33. Permitir escolher pelo menos duas regiões para as quais os arquivos para análise devem ser enviados.
1.9.34. Possuir uma opção que permita a solução identificar automaticamente o caminho com menor latência para envio dos arquivos para análise.
1.9.35. Permitir o administrador criar exceções para aqueles eventos que serão considerados falsos positivos.
1.9.36. O firewall NGFW deve oferecer relatórios locais referente a todos os eventos registrados pela funcionalidade de Sandbox.
1.9.37. A solução deverá prover uma ferramenta distribuída pelo mesmo fabricante para gerenciamento centralizado de ambos os firewalls NGFWs adquiridos pela contratante.
1.9.38. A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar políticas de gerenciamento para um ou mais equipamentos e aplicá-los todos de uma única vez.
1.9.39. As políticas de configurações devem ter no mínimo as seguintes opções:
- Proteção e políticas de acesso web
- Controle de aplicativos
- IPS
- VPN
- E-mail
- Firewall

1.9.40. A solução deverá oferecer funcionalidade que permita o administrador criar templates de configuração, para que o administrador possa aproveitar as mesmas regras para novos firewalls NGFWs.
1.9.41. Deverá haver na dashboard da solução, indicadores que permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.
1.9.42. Possuir múltiplas formas de customização de warning thresholds.
1.9.43. Possuir flexibilização na hora da criação de grupos de firewall NGFWs gerenciados, sendo possível diferenciá-los como por exemplo: Região, modelo ou outro parâmetro.
1.9.44. Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos, com diferentes funções.
1.9.45. Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realiza das caso necessário.

1.10. ANÁLISE E MONITORAMENTO POR INTELIGENCIA ARTIFICIAL

1.10.1. O serviço de firewall deverá ter disponível API's de comunicação para integração com inteligência artificial voltada a cibersegurança.
1.10.2. A inteligência artificial deverá atender todos os equipamentos de firewall e ter compatibilidade com a estrutura ATIVO/ATIVO de firewall.
1.10.3. A inteligência artificial deverá monitorar todas as ações e regras de firewall para levantamento dos dados referentes as configurações executadas medindo o seu nível de efetividade.
1.10.4. Integrar-se aos sistemas de logs do firewall para coletar, analisar e correlacionar eventos de segurança.
1.10.5. A criação de logs deverá ser em tempo real.
1.10.6. Atuar como uma plataforma centralizada para gerenciar várias instâncias de firewalls, oferecendo visibilidade de toda a infraestrutura de segurança.
1.10.7. Em resposta a eventos ou ameaças detectadas, a solução pode disparar ações automáticas no firewall, como bloqueio de IPs, isolamento de dispositivos, ou alterações nas regras de firewall para mitigar riscos.
1.10.8. Deverá ajudar a configurar e gerenciar as políticas de segurança no firewall, permitindo ajustes em tempo real de acordo com as necessidades da organização.
1.10.9. Através da integração com o firewall, a solução deverá oferecer um painel de monitoramento em tempo real, com relatórios detalhados sobre o tráfego de rede, ataques detectados e atividades suspeitas.
1.10.10. Deverá identificar vulnerabilidades de segurança em dispositivos na rede e sugerir ou aplicar correções baseadas nas configurações do firewall.
1.10.11. Quando integrada com a proteção de firewall deverá entregar uma abordagem de segurança mais robusta, correlacionando eventos e tomando medidas mais eficazes para a proteção da rede em tempo real.

1.10.12. Integração com as funcionalidades de prevenção de intrusões (IPS) e proteção contra malware, para uma resposta rápida a ameaças emergentes.

1.11. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

1.11.1. Deverão ser instalados e configurados os itens físicos e lógicos seguindo os padrões e melhores práticas recomendadas na norma NBR ISO/IEC 27002 e conforme critérios definidos pela contratante;

1.11.2. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

1.11.3. Prestar todos os esclarecimentos que lhe forem solicitados, atendendo prontamente a quaisquer reclamações;

1.11.4. Fornecer toda mão de obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;

1.11.5. Instalação física de todos os equipamentos em Rack disponibilizado no local de instalação;

1.11.6. Os equipamentos devem ser configurados em alta disponibilidade, no modo ativo/ativo, dois equipamentos funcionando simultaneamente e em caso de falha o outro continue em operação;

1.11.7. Deverá migrar ou executar configurações similares às configurações atuais implementadas no firewall, atualmente em produção na contratante. A Contratada, além de apontar Marca e Modelo do Firewall, deverá apresentar o projeto de migração completo do Firewall atual para o novo Firewall. Não será aceito um programa automatizado de importação de Regras, especialmente para Firewall com arquitetura diferente da tecnologia atual.

1.11.8. O projeto deve levar em conta a diferença de arquiteturas e demonstrar a preservação das políticas através das camadas.

1.11.9. O equipamento deve estar com firmware e/ou software na versão mais recente e estável recomendada pelo fabricante da solução;

1.11.10. A empresa quando contratada deverá elaborar um plano de implantação junto a Universidade Municipal de São Caetano do Sul, contendo a descrição de atividades a serem desenvolvidas, relatórios e diagramas com dados relevantes para efeito decisório, responsáveis pelas atividades, cronograma de implementação, compondo o documento denominado “Projeto Executivo” tendo a visibilidade completa do projeto e seus status evolutivos. O documento deve ser entregue para a Contratante antes do início da instalação, em até 10 dias úteis a partir do 1º dia útil subsequente a assinatura do contrato. O Gestor do contrato analisará o documento e dará o aceite em um prazo máximo de 02 dias úteis. Havendo necessidade de adequações a empresa terá um prazo máximo de 02 dias úteis para apresentar o projeto readequado, que será reavaliado pelo Gestor para aprovação, em um prazo máximo de 01 dia útil.

1.11.11. Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno nas melhores práticas de configuração do produto e fabricantes;

1.11.12. As senhas configuradas no ambiente durante a instalação deverão ter requisito mínimo de 08 (oito) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;

1.11.13. Os profissionais técnicos quando em serviço na Universidade Municipal de São Caetano do Sul deverão apresentar documento de identificação com foto e identificação da empresa com os seguintes:

- RG/CNH;
- Estar devidamente uniformizado para identificação da empresa Contratada.

1.11.14. A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente.

1.12. MONITORAMENTO

1.12.1. O serviço de monitoramento deverá ser composto de tecnologia que seja totalmente apartada do ambiente computacional e de servidores da Contratante.

1.12.2. A Contratada deverá disponibilizar um switch de 8 portas ou superior, para configurar as conexões de rede necessárias para o monitoramento do ambiente sem a necessidade de utilizar os switches da Contratante.

1.12.3. O switch deverá conter no mínimo os seguintes recursos:

- Capacidade de comutação: 20 Gbps.
- Tabela de endereços MAC no mínimo de: 8.000 mil.
- Memória interna de no mínimo: 256 MB.
- Memória Flash mínima de 32 MB
- Buffer de pacote mínimo de 512 kb.
- Suportar até 256 VLANS simultaneamente e 4.000 mil Ids de VLAN.
- Interface das 8 portas em 10/100/1000 BASE-T ou superior.
- SFP de 1GB no mínimo de 2 Interfaces.
- Interruptor de liga e desliga com entrada DC-in
- Deverá ser 110w.

1.12.4. A Contratante não vai disponibilizar hardware ou software para que a Contratada realize o monitoramento.

1.12.5. Caso o hardware do monitoramento apresente alguma falha, a Contratada terá o prazo de até 1 hora para realizar a substituição nas unidades do Campus Barcelona, Centro, Centro 2, Conceição, e Lato Sensu (Manoel Coelho).

1.12.6. Caso o hardware do monitoramento apresente agulha falha, a Contratada terá o prazo de até 5 horas para realizar a substituição na unidade Campus Itapetininga.

1.12.7. A Contratante não será responsável por armazenar hardware ou software para a substituição.

1.12.8. A fonte de carregamento e gerenciamento de energia deverá ser conectada através da porta tipo-C.

1.12.9. A Contratante não disponibilizará recursos computacionais para a instalação do sistema de monitoramento.

1.12.10. O recurso tecnológico poderá consumir até uma tomada do rack com o tipo padrão NBR 14136 de três pinos.

1.12.11. O recuso tecnológico deverá ser acompanhado com uma fonte de 100/240 VA, padrão NBR 14136 de três pinos, com botão que tenha a possibilidade de ligar e desligar o recurso energético da fonte, deverá entregar 5V de 3000mA e o fio de conexão com a fonte de energia não deverá ser superior a 100cm.
1.12.12. Deverá possuir uma entrada do tipo RJ-45 com a velocidade de Gigabite 10/100/1000.
1.12.13. Deverá possuir 2 entradas USB 2.0.
1.12.14. Deverá possuir 2 entradas de USB 3.0.
1.12.15. Deverá possuir 2 entradas Micro HDMI 2.0.
1.12.16. O recurso tecnológico de monitoramento deverá ter suporte para sistema operacional Linux.
1.12.17. O recurso tecnológico deverá ser um dispositivo para que monitore toda a infraestrutura contratada neste termo de referência.
1.12.18. A comunicação com o datacenter deverá ser feita através do protocolo de comunicação TCP.
1.12.19. O recurso tecnológico deverá possuir um cooler para que ele consiga realizar a dissipação de calor assim evitando qualquer tipo de impacto no serviço de monitoramento.
1.12.20. O recurso tecnológico deverá possuir furação para que a dissipação de calor seja mais eficiente;
1.12.21. O recurso tecnológico deverá possuir o armazenamento em MicroSD de no mínimo 64gb;
1.12.22. A Contratada ficará responsável em realizar a entrega do recurso tecnológico juntamente com as respectivas licenças do sistema operacional e softwares de segurança como licença contra-ataques cibernéticos, backup do sistema operacional e até mesmo monitoramento do sistema tecnológico.
1.12.23. A solução deve ser concebida nativamente sobre uma arquitetura distribuída de múltiplos agentes de software autônomos, sendo no mínimo 6 agentes de IA, não podendo ser um mero agregado de ferramentas de terceiros.
1.12.24. Cada agente deve ser um processo de baixo impacto (low footprint) em termos de consumo de CPU e memória, capaz de operar de forma contínua no ativo (servidor, computador, etc.) sem degradar sua performance.
1.12.25. Os agentes de IA utilizaram o seu conhecimento para orquestrar atividade nos ativos, de acordo com a demanda as atividades serão auditadas, executadas e documentadas.
1.12.26. A IA e os seus agentes devem ser o motor de orquestração central, utilizando um modelo de Gráfico de Conhecimento (Knowledge Graph) para mapear dinamicamente e em tempo real os relacionamentos entre todos os ativos do ambiente (identidades, dispositivos, aplicações, dados, vulnerabilidades, etc.) e organizá-los em um contexto de dados no qual os agentes tenham a capacidade de personalizar a interação do usuário, diminuir a complexidade, aumentar a qualidade e a produtividade.
1.12.27. A plataforma deve ser capaz de, a partir da análise deste gráfico, inferir cadeias de ataque (Cyber Kill Chains) complexas e multivetoriais, correlacionando eventos de baixa relevância que, isoladamente, não seriam considerados ameaças.
1.12.28. A resposta a incidentes deve ser dinâmica e contextual, baseada nas inferências do motor cognitivo, superando a execução de fluxos de trabalho estáticos e lineares.
1.12.29. A solução de segurança com inteligência artificial para detecção e resposta estendida a incidentes na camada de proteção nos servidores, deverá ser totalmente compatível com a estrutura em cloud.
1.12.30. A contratação da prestação dos serviços e a disponibilização da ferramenta deverão atender integralmente aos normativos emitidos pelos órgãos fiscalizadores e de controle competentes, em especial ao disposto na Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).
1.12.31. A plataforma deve contar com agentes da Inteligência Artificial para auxiliar em toda a etapa da investigação.
1.12.32. A plataforma deve disponibilizar comunicação direta por texto com os agentes da Inteligência Artificial
1.12.33. A plataforma deve disponibilizar durante a navegação, interação com a Inteligência Artificial e acesso aos dados investigados.
1.12.34. A plataforma deve utilizar diferentes agentes da Inteligência Artificial para investigação de endpoints, alertas e Inteligência de ameaças.
1.12.35. A inteligência Artificial deve ser capaz de buscar todos os endpoints cadastrados, alertas abertos e vulnerabilidades identificadas na interação por texto e o resultado deve ser retornado em tela.
1.12.36. Os agentes de Inteligência devem ser capazes de correlacionar todos os dados coletados, analisar e fornecer um parecer investigativo sobre quais ações foram e/ou devem ser realizadas.
1.12.37. Deve usar um modelo matemático gerado a partir de aprendizado de máquina para comparar diferentes características de um arquivo executável, de forma estática, para determinar se ele é malicioso.
1.12.38. A plataforma deve ser capaz de detectar vazamentos de dados relacionados à Contratante, indicando o tipo de dado exposto e as datas que ocorreram.
1.12.39. A plataforma através dos agentes da Inteligência Artificial deve ser capaz de reclassificar a pontuação de risco da ameaça de acordo com a técnica explorada e a classificação do ativo;
1.12.40. A plataforma deve ser capaz de se integrar a aplicações e equipamentos da Contratante para enriquecer a detecção e resposta estendida em tempo real;
1.12.41. A proteção deve estar disponível para os sistemas operacionais Windows, Linux e MacOS.
1.12.42. Prevenção de ameaças baseada em comportamento para análise dinâmica de processos em execução.
1.12.43. Prevenção de exploração por técnicas conhecidas de exploits.
1.12.44. Prevenção de exploração baseada em kernel.
1.12.45. Prevenção de ameaças com base em inteligência de ameaças, como hash de arquivos.
1.12.46. Integração automatizada com um serviço de prevenção de malware, baseado em nuvem do próprio fabricante.
1.12.47. A solução deve prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros.
1.12.48. A solução deve ser compatível, no mínimo, com os seguintes sistemas operacionais e distribuição:
- Linux ou Windows.

1.12.49. A solução deve incluir na análise de execução, no mínimo, as seguintes características:
- Táticas e técnicas de acordo com o modelo de ameaças MITRE ATT&CK;
- Caraterísticas comportamentais suspeitas;

- Detalhes do arquivo como nome, hash, tamanho, tipo;
- Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
- Leitura e escrita de arquivos em disco;
- Leitura e alteração de chaves de registro.

1.12.50. Detalhes de processos iniciados durante a execução.
1.12.51. Atualizações transparentes do mecanismo de detecção de ameaças.
1.12.52. Proteção contra malware, ransomware e ataques sem arquivo.
1.12.53. Identificação e prevenção de tentativas de escalonamento de privilégios ao nível de Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux.
1.12.54. Deve permitir gerar alertas das soluções integradas.
1.12.55. Deve permitir a consulta de eventos de forma integrada.
1.12.56. Os usuários locais da solução devem ter uma política de senha que permita, no mínimo as seguintes configurações, alteração no primeiro login e identificação de complexidade de senha.
1.12.57. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless).
1.12.58. No caso de detecção de um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos.
1.12.59. A solução deve disponibilizar o rastreio de detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências.
1.12.60. A solução deve disponibilizar o rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante.
1.12.61. A solução deve disponibilizar o rastreio de tentativas de roubo de credenciais e\ou tentativa de acessos indevidos a recursos chave do sistema operacional.
1.12.62. Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa artefatos, destacando rapidamente índices de comprometimento já conhecidos.
1.12.63. Gerenciamento unificado e centralizado de todas as funções na mesma console de, bem como a instalação e atualização dos agentes.
1.12.64. Detecção de comprometimento: vírus, malware, backdoors, hosts em comunicação com sistemas infectados por botnet, serviços da Web vinculados a conteúdo malicioso.
1.12.65. Frequência de atualização, personalizável por dia, semana ou mês.
1.12.66. Varredura em tempo real de arquivos (gravação, renomeio e leitura) e de processos em memória.
1.12.67. Monitoramento em tempo real para captura de malwares que são executados em memória sem a necessidade de escrever em arquivo.
1.12.68. Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise comportamental, realizado por inteligência artificial.
1.12.69. Solução única para proteção contra malwares e ransomware, com a capacidade de coletar dados de sistemas operacionais e de rede para detecção de eventos maliciosos, sem a obrigatoriedade de criação e ativação de regras manualmente.
1.12.70. A solução deve permitir instalação silenciosa do agente, em sistemas operacionais Windows, através de pacotes MSI e executável EXE.
1.12.71. A solução deverá ser capaz também de analisar ameaças, sem o uso de assinaturas, fazendo esta análise por comportamento.
1.12.72. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações.
1.12.73. A solução deve suportar nativamente a integração com terceiros, sem a necessidade de instalação de recursos adicionais para receber eventos de múltiplas fontes de origem.
1.12.74. A solução deve disponibilizar, informações sobre o número de dispositivos que possuem o agente instalado e a versão do agente.
1.12.75. A solução deve ser capaz de monitorar o serviço de e-mail e domínio para identificar vazamento de dados.
1.12.76. Requisitos de detecção e resposta do agente
1.12.77. A solução não deve ter limitação para recebimento de eventos.
1.12.78. A comunicação entre agente e plataforma deve acontecer através do protocolo TCP porta 443;
1.12.79. O agente deve permitir a sua instalação em sistema operacional Linux Ubuntu 24.04 ou superiores.
1.12.80. A solução deve utilizar criptografia para conexão entre agente e plataforma, no mínimo, TLS 1.3 com AES 256.
1.12.81. A solução deve utilizar criptografia nos dados enviados para a plataforma de gerenciamento, no mínimo, AES 256.
1.12.82. A solução deve utilizar algoritmos de aprendizado de máquina para identificar padrões e comportamentos suspeitos.
1.12.83. A solução deverá ser capaz de bloquear tanto ameaças conhecidas como também as desconhecidas.
1.12.84. O agente deve detectar e proteger o dispositivo mesmo offline.
1.12.85. O agente deve receber atualizações de forma automática.
1.12.86. O agente deve receber as novas assinaturas de segurança em tempo real.
1.12.87. A solução deve utilizar detecção de ameaças por meio de dados e padrões baseados em comportamentos, que se utilizam de motores baseados em aprendizado de máquina para averiguação de arquivos.
1.12.88. O agente deve possuir a funcionalidade de inteligência contra malware.
1.12.89. O agente deve possuir a funcionalidade de inteligência contra ransomware.
1.12.90. O agente deve possuir a funcionalidade de bloqueio de indicadores de comprometimento.
1.12.91. O agente deve disponibilizar na sua interface, os seguintes dados:
1.12.91.1. Nome do usuário logado;
1.12.91.2. Nome do host;
1.12.91.3. Informações de sistema operacional (Build, Plataforma);

1.12.91.4. Estado do equipamento (Online ou Offline);
1.12.91.5. Última data comunicação com a console de gerenciamento;
1.12.91.6. Informações relacionadas à rede (IP, DNS, DHCP).
1.12.92. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela contratada.
1.12.93. A solução deve operar em tempo real, monitorando e bloqueando as ameaças.
1.12.94. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes.
1.12.95. A solução deve fornecer a capacidade de executar análises de estações de trabalho/servidores sem a necessidade de interagir com o usuário. Essa capacidade deve ser centralizada e transparente para o usuário.
1.12.96. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger e atualizar.
1.12.97. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho.
1.12.98. A solução deve ser capaz de fazer análise avançada e utilizar algoritmos de aprendizado de máquina, mesmo que sem conexão ao servidor de gerenciamento.
1.12.99. Consulta APIs: Capacidade de extrair dados de segurança e eventos para integração, utilizando os protocolos SSH, HTTP, SNMP e Syslog em todos os itens fornecidos dentro da solução proposta.
1.12.100. A solução deve disponibilizar um agente instalável e compatível com sistemas operacional, Windows, Linux e MacOS. Com a capacidade de detectar, coletar e enviar a plataforma, comportamentos maliciosos de aplicações que estão sendo executadas no sistema operacional.
1.12.101. A solução deve disponibilizar um coletor com capacidade de executar consultas de coleta de eventos e detecção de ação maliciosas em suas integrações, mesmo se houver indisponibilidade de conectividade.
1.12.102. Atualizações regulares e automáticas de binários e base de dados de segurança.
1.12.103. O agente deve ser compatível com o sistema operacional Linux Ubuntu 24.04 ou superiores.
1.12.104. A solução deve suportar a integração baseada em agente e autenticação.
1.12.105. A solução deve permitir o recebimento de eventos por múltiplos coletores.
1.12.106. A solução deve identificar os eventos por integração e agente.
1.12.107. A solução deve permitir a classificação de severidade, quando cadastrado o dispositivo.
1.12.108. Quanto ao armazenamento
1.12.108.1. A solução deve prover no mínimo 2TB de armazenamento para retenção dos eventos coletados e normalizados pela solução, sem custo adicional ou necessidade de fornecimento de hardware para armazenamento pela Contratante.
1.12.108.2. O evento armazenado pela solução, bem como hardware necessário para tal, é de responsabilidade da Contratada em armazenar em datacenter.
1.12.108.3. Solução deve ter a capacidade de permitir que a Universidade USCS modifique o período de armazenamento de eventos de Windows, Linux e Firewall de forma independente e através de plataforma gráfica disponibilizada pela solução proposta pela Contratada.
1.12.109. Quanto a Relatórios e Dashboards.
1.12.109.1. Visualização de Dados.
1.12.109.2. Painéis de controle para visualização em tempo real de incidentes e status de segurança.
1.12.109.3. Relatórios sobre incidentes, tendências de segurança e desempenho do sistema, exportando em formatos pdf, csv e html.
1.12.109.4. A solução deve ter capacidade de enviar relatórios através dos protocolos SMTP, HTTP, SFTP e ter integração com soluções de colaboração.

1.13. RELÁTORIOS

1.13.1. Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, com relatório de chamados referentes ao serviço descrito nesse lote:
1.13.2. Categoria do chamado;
1.13.3. Usuário;
1.13.4. Ativos relacionados;
1.13.5. Data de abertura e fechamento;
1.13.6. Status;
1.13.7. Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):
1.13.8. Disponibilidade;
1.13.9. Consumo de hardware (CPU, memória, disco, consumo de banda);
1.13.10. Alertas e erros.

1.14. SUPORTE TÉCNICO

1.14.1. Os serviços de suporte técnico especializado, deverão contemplar toda a solução e infraestrutura de segurança contidas neste Termo de Referência.

1.14.2. A USCS poderá abrir chamados de manutenção através de chamada telefônica para número com DDD (11), central de atendimento via navegador (WEB) ou correio eletrônico sem a necessidade prévia consulta e/ou qualquer liberação por parte da Contratada;
1.14.3. O atendimento técnico remoto deverá ocorrer 24 horas por dia.
1.14.4. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas de hardware e/ou software;
1.14.5. Toda falha e indisponibilidade no ambiente ocasionado por falhas físicas nos equipamentos (hardware) será de plena responsabilidade da Contratada.

1.14.6. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos;

1.14.7. Será de responsabilidade da Contratada manter o pleno funcionamento das políticas de segurança da solução.

1.14.8. Deverá monitorar diariamente, os relatórios de segurança gerados ao concluir as tarefas, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da Contratada efetuar correção ou ajuste técnico para a normalização dele, garantindo o pleno funcionamento da solução;

1.14.9. A Contratada deverá ser responsável por executar as restaurações do ambiente.

1.14.10. A empresa Contratada se responsabilizará pelas despesas com material de escritório, reprodução de documentos (cópias, etc.) e materiais diversos, que forem necessários à execução dos serviços de manutenção dos serviços e pelos seus profissionais;

1.14.11. A Contratada deverá realizar atendimentos remotos à equipe da Diretoria de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul, a partir de solicitações recebidas dos técnicos ou gestores do instrumento de contrato a ser celebrado com o vencedor do certame, via sistema de atendimento, telefone ou correio eletrônico;

1.14.12. Os atendimentos presenciais terão o prazo de até 1 hora para iniciar o atendimento nas unidades do Campus Barcelona, Centro, Centro 2, Conceição, e Lato Sensu (Manoel Coelho) e após a constatação técnica da Contratada.

1.14.13. O atendimento presencial terá o prazo de até 5 horas para iniciar o atendimento na unidade Campus Itapetininga após a constatação técnica da Contratada.

1.14.14. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados;

1.14.15. Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências;

1.14.16. Manter o ambiente de segurança sempre atualizado em com as melhores práticas aplicadas;

1.14.17. A Contratada deverá garantir que os profissionais designados para atendimento técnico serão capacitados;

1.14.18. A garantia de tempo de resposta será realizada conforme critérios de prioridades a seguir:

Classe	Descrição	Início do Atendimento em Até
1	Serviço indisponível	1 hora
2	Suporte técnico de maior impacto	4 horas
3	Suporte técnico com menor impacto	8 horas
4	Manutenção preventiva	Programada

1.14.19. O acordo de nível de serviço **(SLA)** para suporte técnico deverá obedecer ao seguinte escopo, respeitando-se as particularidades de cunho localização geográfica das Unidades.

PRIORIDADE	DESCRIÇÃO
1 (Emergencial)	O serviço está fora de operação ou há um impacto crítico nas operações.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações que sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

1.14.20. As horas para primeiro atendimento e resolução de incidentes são horas corridas e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

1.14.21. Caso seja identificado que o Serviço de Segurança se encontra indisponível por causa de soluções de terceiros, link de internet, indisponibilidade de switch, energia elétrica, roteadores, firewall, problemas de hardware/infraestrutura de TI ou qualquer serviço que interligue as unidades, será de responsabilidade da Contratada em realizar a detecção e resolução do problema.

1.14.22. A Contratada deverá disponibilizar e gerenciar os atendimentos técnicos da Universidade Municipal de São Caetano do Sul através de portal de gerenciamento de atendimentos com acesso através de navegador web;

1.14.23. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central;

1.14.24. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;

1.14.25. A Contratada deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento;

1.14.26. A Universidade USCS deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail;

1.14.27. O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da empresa Contratada, sendo essa responsável por sua atualização e manutenção;

1.14.28. A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;

1.14.29. O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;
1.14.30. A Contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela USCS;
1.14.31. Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;
1.14.32. Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a Universidade USCS;
1.14.33. O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a Contratante;
1.14.34. Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;
1.14.35. A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";
1.14.36. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;
1.14.37. Deverá ser possível a criação de grupos de usuários na solução;
1.14.38. A solução disponibilizada pela empresa Contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.
1.14.39. Relatórios Mensais, durante o período do contrato
1.14.40. Relatório de Chamados:
1.14.41. Categoria do chamado;
1.14.42. Usuário;
1.14.43. Ativos relacionados;
1.14.44. Data de abertura e fechamento;
1.14.45. Status;
1.14.46. O suporte técnico deverá ter os seguintes canais de atendimento: Suporte Telefônico, E-mail e Sistema online de chamados, todos em português do Brasil;
1.14.47. A empresa Contratada deverá sempre disponibilizar versões mais recentes dos softwares sem ônus financeiro para a Universidade;

1.15. MANUTENÇÃO PREVENTIVA DA SOLUÇÃO DE INTELIGENCIA ARTIFICIAL

1.15.1. A manutenção preventiva será destinada a atualizar os componentes de software (atualização tecnológica), conforme definições nesse documento, e a realizar quaisquer operações que evitem uma parada total ou parcial da solução.
1.15.2. ~~A~~ USCS, através de sua equipe técnica de Tecnologia da Informação, observará o desempenho do sistema contratado e, caso necessário, solicitará à Contratada a manutenção preventiva para viabilizar o melhor desempenho da solução.
1.15.3. A manutenção preventiva está inclusa no suporte técnico da solução, sendo prestada pela Contratada sem qualquer ônus adicional para a Contratante.
1.15.4. Durante a manutenção preventiva, a Contratada deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta.
1.15.5. Durante o período de suporte técnico deverá ser realizada a atualização de qualquer outro software constituinte da solução para as versões mais recentes, sem ônus adicional para a Universidade USCS.
1.15.6. A manutenção corretiva será destinada a remover erros ou falhas apresentadas pelos componentes de software da solução contratada.
1.15.7. Como erro ou falha entende-se a geração de resultado diferente do previsto. Para a resolução desses erros, é necessária a intervenção técnica especializada ou mesmo até a substituição de seus componentes por parte da empresa Contratada.
1.15.8. A manutenção corretiva após o diagnóstico (determinação da origem da falha) deverá ser realizada por meio de ajustes, consertos ou substituição dos elementos que apresentam problemas, restabelecendo a solução suas condições normais de funcionamento ou operação, conforme as especificações do fabricante.
1.15.9. Entende-se como diagnóstico à compilação e análise de informações para definição da causa de um problema.
1.15.10. Entende-se como Recuperação da Disponibilidade a execução de atividades que permitem restabelecer o funcionamento da solução.
1.15.11. A comprovação de isenção de responsabilidade se dará pela apresentação de relatório técnico circunstanciado dos elementos da solução contratada, e pelas demais informações consideradas necessárias pela Contratada para embasar a justificativa.
1.15.12. Tomar todas as providências necessárias para que seus funcionários, representantes e/ou contratados observem os regulamentos, normas e instruções de segurança da informação e Comunicações pela USCS, quando estiverem executando serviços.
1.15.13. A Contratada deve comprometer-se a manter informações confidenciais no mais estrito sigilo sobre todos os dados, configurações, processos, fórmulas, rotinas e quaisquer outros objetos que sejam disponibilizados pela USCS à Contratada, para a realização dos trabalhos. Compromete-se a não copiar, não usar em seu próprio benefício, nem revelar ou mostrar a terceiros, nem divulgar tais informações, no território brasileiro ou no exterior, sob pena prevista em lei. Só os representantes e prepostos, devidamente autorizados entre as partes, cuja avaliação das informações confidenciais seja necessária e apropriada, para os propósitos especificados em contrato, terão acesso às mesmas.
1.15.14. Prestar os esclarecimentos necessários a Contratante, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.
1.15.15. Requisitos sociais, ambientais e culturais.
1.15.16. Sistema e todos os seus módulos deve ser desenvolvido/disponibilizado de forma compatível para as características do Brasil quanto a aspectos de interface gráfica, linguagem, legislação, costumes, apresentação, funcionalidades, telas e relatórios. Deve também possuir manuais de usuário online, com possibilidade de impressão, e documentação técnica do software em idioma português do Brasil ou inglês.

2. Especificações e Exigências Aplicadas ao Lote 02

Com relação ao **lote 02**, a Universidade Municipal de São Caetano do Sul pretende satisfazer a necessidade específica relacionada ao fornecimento de toda a infraestrutura em nuvem privada, necessária para equacionar a demanda de serviço de hospedagem em data center e hosting, gestão e monitoramento cloud computing de sua estrutura computacional, incluindo máquinas virtuais, link de acesso, segurança da informação, migração de suas aplicações e base de dados, bem como suporte técnico e monitoramento 24x7 da infraestrutura virtual a partir da contratação de empresa detentora desse *Know-how* por período de 24 meses.

Abaixo descreve-se a relação de serviços integrantes desse lote, bem como suas especificidades.

	Item	Descrição	Quantidade em meses
LOTE 02		SERVIÇO DE DATA CENTER HOSTING.	24
		SERVIÇO DE SUPORTE TÉCNICO.	24
		SERVIÇO DE MONITORAMENTO (NOC)	24
		SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	01

2.1. DATA CENTER HOSTING

2.1.1. A estrutura computacional em hosting deverá respeitar rigorosamente este termo de referência.
2.1.2. Os equipamentos ofertados devem ser novos, sem uso anterior.
2.1.3. O serviço de data center in cloud deverá possuir dois servidores totalmente compatíveis com alta disponibilidade.
2.1.4. Todo o licenciamento do ambiente em cloud deverá ser responsabilidade da Contratada.
2.1.5. Todo o licenciamento disponibilizado para esse projeto deverá ser da Microsoft.
2.1.6. Os dois servidores deverão ser iguais, do mesmo fabricante, sem modificações ou alteração do escopo de configuração.
2.1.7. Ambos os servidores deverão possuir compatibilidade com as configurações de tecnologia em alta disponibilidade.
2.1.8. As especificações do servidor tanto como o modelo do servidor, no ato da proposta comercial, deverão ser apresentadas para a validação computacional.

2.2. ESPECIFICAÇÕES DO PROCESSADOR

2.2.1. Cada servidor deverá ter no mínimo 2 (dois) processadores.
2.2.2. Cada processador deverá ter 16 Core.
2.2.3. Cada processador deverá ter 32 Threads.
2.2.4. Cada processador deverá ter no mínimo 3.0GHz.
2.2.5. Cada processador deverá ter no mínimo 64MB de cache.
2.2.6. O processador deverá estar em linha de produção fora do prazo de fim de vida/suporte técnico.
2.2.7. Deverá suportar virtualização.

2.3. ESPECIFICAÇÕES DA MEMORIA RAM

2.3.1. Cada servidor deverá ter no mínimo 2 (dois) processadores.
2.3.2. Cada servidor ter 1TB de memória RAM disponível para a utilização.
2.3.3. A velocidade da memória RAM deverá ser DDR5 RDIMM 5600MHz.

2.4. ESPECIFICAÇÕES DO ARMAZENAMENTO

2.4.1. Os servidores deverão atender os requisitos de armazenamento:
2.4.2. Deverá ter no mínimo o espaço de 400GB de disco SSD em RAID-1;
2.4.3. Deverá ter no mínimo o espaço em disco de 7TB com a taxa de escrita em até 10k em tecnologia SAS, em RAID-5;
2.4.4. Deverá ter no mínimo o espaço em disco de 6TB sendo a tecnologia SSD SATA em RAID-5.

2.5. COMUNICAÇÃO ENTRE OS SERVIDORES

2.5.1. Os servidores deverão se comunicar em 40GB.
2.5.2. A conectorização de comunicação obrigatoriamente deverá ser em QSFP.

2.6. CARACTERÍSTICAS FÍSICAS DO DATA CENTER

2.6.1. O Data Center in cloud deverá ser localizado no **Estado de São Paulo** para evitar alta lentidão.
2.6.2. Será de responsabilidade da Contratada implementar e configurar toda a estrutura contratada pela Universidade Municipal de São Caetano nesse termo de referência (lote 02).
2.6.3. O Data Center deverá atender no mínimo no que se refere as certificações Tier III ou ISO27001 ou SOC 2 Type 2;
2.6.4. O licenciamento e operação do ambiente em nuvem será de total responsabilidade da empresa vencedora do certame a ser contratada;
2.6.5. A Contratada deverá garantir a segurança da informação dos dados e estrutura em nuvem que irá hospedar os dados da USCS.
2.6.6. O Data Center deverá ter a estrutura de firewall, em alta disponibilidade e que supra a necessidade de transferência de dados.
2.6.7. O ambiente de firewall não poderá ter limite de conexões VPN.
2.6.8. Não será aceito nenhuma appliance de firewall genérica.
2.6.9. Não será aceito nenhuma appliance de firewall sem fabricante que possa desenvolver atualizações e vacinas.
2.6.10. O ambiente deverá ter a tecnologia de duplo fator de autenticação para acessar o ambiente computacional em cloud.
2.6.11. As instalações físicas do data center deverão ter os seguintes itens:

- Sistema de piso elevado, com vias independentes de cabos de energia, lógicos e óticos;
- Deverá possuir vias de energia elétrica e lógica em alta disponibilidade;
- Sistema de proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento.

2.6.12. A estrutura de energia elétrica do data center deverá atender aos seguintes requisitos:
- Alimentação elétrica redundante;
- Total independência no fornecimento de energia na eventualidade de falha na subestação que atende ao data center;
- Solução de grupo gerador redundante e independente (n+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia e com capacidade mínima de funcionamento por 72 horas com combustível local;
- Mínimo de 2KVAs nominais;
- Alimentação elétrica redundante e independente para os equipamentos da solução.

2.6.13. O Data Center que alocará o ambiente computacional da USCS e deverá atender os seguintes requisitos de climatização:
- Sistema de climatização com controles de temperatura, umidade relativa do ar e filtros de poeira;
- Sistema de climatização redundante (n+1), refrigerado por formas diferentes;
- Temperatura constante de 20ºC +/- 2ºC e umidade relativa do ar constante de 50% +/-10%.

2.6.14. O Data Center que alocará o ambiente computacional da USCS e deverá atender os seguintes requisitos de proteção contra incêndio:
- Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);
- Sistema automático de extinção de incêndios, baseado em agentes gasosos não poluentes, com ação baseada na quebra das moléculas de Oxigênio, do tipo FM200 e/ou FE227, ou equivalente, não nocivos aos equipamentos e seres humanos e que atenda a padrões internacionais;
- Sistema de detecção de incêndio por sensores termovelocimétricos para a sala dos servidores do data center, tipo VESDA, ou equivalente; possuir dispositivos de detecção precoce de incêndio pela análise do superaquecimento de cabos ou hardwares que sejam de maior sensibilidade que os tradicionais detectores de fumaça;
- Possuir sistema de detecção de incêndio por sensores termovelocimétricos para os ambientes de servidores e de armazenamento de dados;
- Possuir os componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.

2.6.15. O Data Center que alocará o ambiente computacional da USCS e deverá possuir os seguintes requisitos de segurança física:
- Disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;
- Mecanismos efetivos de controle de entrada e saída de pessoas que acessem e façam uso do IDC, bem como de registros passíveis de posterior pesquisa;
- Capacidade de cadastro remoto de usuários para acesso ao data center;
- Deverá possuir a capacidade de cadastro de novo usuário local com permissão do administrador;
- Acesso ao local através de leitura biométrica;
- Possuir alerta por SMS e e-mail em tempo real de acesso ao ambiente;
- Arquivar as imagens gravadas pelas câmeras de vídeo de segurança por pelo menos 30 (trinta) dias;
- O Datacenter deverá possuir vigilância patrimonial 24 horas por dia, 7 dias por semana, 365 dias por ano, permitindo apenas a entrada de pessoas autorizadas e devidamente identificadas;
- Possuir metodologia para classificação e controle de ativos e de acessos ao ambiente do Datacenter;
- Acondicionar equipamentos e mídias geradas no ambiente do Datacenter, livres de riscos físicos;
- Possuir rígido controle de acessos aos equipamentos do Datacenter, mesmo por pessoas credenciadas pela Contratante;
- Disponibilizar mecanismos efetivos de controle de entrada e saída de pessoas, que acessam ou façam uso do Datacenter, com leitores biométricos ou cartões magnéticos individuais;
- Possuir travas eletrônicas que, de acordo com a política de segurança estabelecida para o Datacenter, a dívida em regiões com níveis de restrição diferenciados;
- Possuir sistema de detectores de movimento no ambiente.

2.7. COMUNICAÇÃO COM A INTERNET E REDUNDANCIA

2.7.1. Deverá ser disponibilizado pela contratada 1 link de internet para gerenciamento de no mínimo de 50MB dedicado.

2.7.2. Será fornecido um link da REDNESP (ANSP), que deverá ser instalado e configurado conforme as especificações técnicas definidas no **Item 2.7**.

2.7.3. A Contratada deverá disponibilizar no data center ofertado toda a estrutura para receber o link da Contratante que deverá ser interligado com o link disponibilizado pela FAPESP gratuitamente para acesso à internet, sendo, portanto, um ponto da rede de acesso da Rednesp (ANSP);

2.7.4. A Contratada deverá a interligar o ambiente de nuvem privada da Contratante com a rede da Rednesp (ANSP).

2.7.5. É de total responsabilidade da Contratada toda a infraestrutura necessária para realizar a interligação da unidade e data center destacado.

2.7.6. A Contratada deverá prover a conectividade entre a sala de cross do Data Center e o cage da Rednesp (ANSP), bem como com o rack ou cage (gaiola) onde estarão hospedados os servidores virtuais da Contratante.

2.7.7. A Contratada deverá interligar a unidade localizada na Avenida Goiás, 3400, Barcelona, São Caetano do Sul, São Paulo com o ambiente em cloud hospedado através de fibra ótica, com velocidade mínima de 1Gb.

2.7.8. A navegação na internet da unidade citada acima deverá ser através do link disponibilizado pela FAPESP, utilizando a interligação de fibra ótica, conforme item anterior.

2.8. BACKUP DO AMBIENTE COMPUTACIONAL

2.8.1. Toda a estrutura computacional em nuvem deverá ter backup diário.

2.8.2. O Backup deverá ser executado todos os dias e a cada 4 (quatro) horas.

2.8.3. Por dia o backup deverá ter 6 pontos de restauração.

2.8.4. O backup mensal deverá ter no mínimo 180 pontos de restauração.

2.8.5. A retenção do backup deverá ser de no mínimo por 1 (um) ano.
2.8.6. O licenciamento da solução deverá cobrir a solução de Armazenamento e Compartilhamento de arquivos em Windows, presente neste documento, pelo período do contrato;
2.8.7. A solução deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução, incluindo retorno (rollback) de réplicas e replicação até a infraestrutura virtualizada.
2.8.8. O software de backup deverá cobrir pelo menos 30 máquinas virtuais.
2.8.9. A solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.
2.8.10. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização Hyper-V, conforme Contratada.
2.8.11. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes.
2.8.12. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto.
2.8.13. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
2.8.14. Deverá prover a deduplicação e compressão das máquinas virtuais diretamente e durante a operação de backup.
2.8.15. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.
2.8.16. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.
2.8.17. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.
2.8.18. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreio de blocos modificados" (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
2.8.19. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:
- Diretamente através de Storage Area Network (SAN);
- Diretamente do storage, através do hypervisor I/O (Virtual Appliance);
- Mediante uso da rede local (LAN);
- Diretamente do snapshot do storage onde os dados das VMs estejam armazenados; (para Netapp, HPE 3Par ou EMC VNX).

2.8.20. Deverá proporcionar um controle centralizado de implementação distribuída, para isso deverá incluir uma console web, integrada ou não, que possibilite uma visão consolidada de sua arquitetura distribuída e conjunto de múltiplos servidores de proteção (backup), relatórios centralizados, alertas consolidados e restauração de autosserviço de máquinas virtuais no nível de sistema de arquivos (granular), com delegação de permissões sobre máquinas virtuais individuais.
2.8.21. Deverá poder manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço.
2.8.22. Deverá contar com tecnologia de deduplicação também para o ambiente de máquinas virtuais para gerar economia de espaço de armazenamento no repositório de backups sem a necessidade de hardware de terceiros (appliance deduplicadora).
2.8.23. Deverá proporcionar proteção quase contínua de dados (near-CDP), permitindo a minimização dos Objetivos de Pontos de Recuperação (RPO).
2.8.24. Deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do arquivo de backup, armazenado no repositório de backup de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do backup, os quais obrigatoriamente deverão estar "deduplicados" e também "comprimidos".
2.8.25. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.
2.8.26. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.
2.8.27. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar
2.8.28. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup.
2.8.29. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
2.8.30. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle.
2.8.31. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.
2.8.32. Deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.
2.8.33. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2010 sp1, 2013 e superiores, possam recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma.

2.8.34. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft Active Directory, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
2.8.35. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, tais como Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
2.8.36. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2010, sem a necessidade de agentes. (recuperação granular).
2.8.37. Deverá incluir ferramentas de recuperação de elementos individuais para Microsoft Exchange 2010-SP1 em diante, sem que seja necessário inicializar a máquina virtual a partir do backup e que possa ser extraído a frio (ex. mensagens, tarefas, contatos, etc.) e sem requerer infraestrutura intermediária (staging), fazer busca rápidas no servidor de e-mail
2.8.38. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, gerando confiabilidade de 100% na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.).
2.8.39. Deverá permitir criar uma cópia da máquina virtual de produção, para criação de ambiente de homologação, teste, QA, etc; em qualquer estado anterior para a resolução de problemas, provas de procedimentos, capacitação, entre outros. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only).
2.8.40. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO3 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS.
2.8.41. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.
2.8.42. Deverá ser fornecida com a funcionalidade de acelerar a rede "WAN" para geração de cópia ou replicação das máquinas virtuais, sem utilização de agentes, nem configurações de rede especiais.
2.8.43. Deverá incluir suporte para VMware vCloudDirector com visibilidade integrada da infraestrutura vCD no console de backup, fazendo backup de meta-dados e dos atributos associados com vApps e VMs, permitindo a recuperação diretamente ao vCD.
2.8.44. Deverá incluir um plug-in para VMware vSphere Web Client, afim de permitir o monitoramento da infraestrutura de backup diretamente do vSphere Web Client, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup.
2.8.45. Deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:
- Microsoft Active Directory Server 2008 R2 em diante
- Microsoft Exchange Server 2010-SP1 em diante;
- Microsoft SQL Server 2008 SP4 em diante;
- Microsoft Sharepoint 2010 em diante;
- Oracle Database 11g, 12c, 18c, 19c e 21c.

2.8.46. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados.
2.8.47. Deverá regular de forma dinâmica e parametrizável, a exigência sobre os sistemas protegidos, de forma tal, que se possa definir limites de utilização de performance em discos para diminuir o impacto na infraestrutura de produção, durante as atividades de backup.
2.8.48. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência.
2.8.49. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação.
2.8.50. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.
2.8.51. Deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de backup que esteja alojado em um provedor de serviços na nuvem (backup ou replicação na nuvem - cloud providers).
2.8.52. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas;
2.8.53. Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:
- Microsoft Windows;
- Linux;
- Pastas compartilhadas;
- Appliances de duplicadoras.

2.8.54. Suportar servidores proxy de backup virtuais ou físicos para backup de máquinas virtuais;
2.8.55. Deve estar homologado para o Oracle Database 11g e 12g nos sistemas operacionais Windows ou Linux sem a necessidade de instalação de agentes;
2.8.56. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;
2.8.57. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a Universidade Municipal de São Caetano do Sul se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem incorrer em nenhum ônus adicional decorrente dessa decisão.
2.8.58. Além do armazenamento em nuvem, o backup deverá ter uma unidade com imutabilidade, realizando o armazenamento e podendo ser solicitado a qualquer momento.
2.8.59. A solicitação de recuperação do backup não poderá ter custos adicionais por taxa de transferência.

2.9. INSTALAÇÃO E CONFIGURAÇÃO DO AMBIENTE COMPUTACIONAL

2.9.1. Deverão ser instalados e configurados os itens lógicos seguindo os padrões e melhores práticas recomendadas conforme critérios definidos pela contratante;

2.9.2. O ambiente computacional deverá ser capaz de acomodar até **30 máquinas virtuais** com o sistema operacional, sendo de responsabilidade da Contratante fornecer o licenciamento.

2.9.3. Os recursos alocados para a virtualização deverão ser apresentados pela Contratante não ultrapassando o limite contratado.

2.9.4. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

2.9.5. Prestar todos os esclarecimentos que lhe forem solicitados, atendendo prontamente a quaisquer reclamações;

2.9.6. Entregar toda mão de obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;

2.9.7. Os equipamentos de firewall do data center em cloud devem ser configurados em alta disponibilidade, no modo ativo/ativo, dois equipamentos funcionando simultaneamente e em caso de falha o outro deverá assumir a operação;

2.9.8. Deverá migrar ou executar configurações similares às configurações atuais implementadas no ambiente em cloud, atualmente em produção.

2.9.9. O ambiente deverá ser entregue com os softwares e atualizações mais recentes disponibilizados pelo fabricante tanto quanto, ambiente de conectividade via firewall, sistemas operacionais, firmwares e drives para que se obtenha total compatibilidade.

2.9.10. A empresa quando contratada deverá elaborar um plano de implantação junto a Universidade Municipal de São Caetano do Sul, contendo descrição de atividades a serem desenvolvidas, relatórios e diagramas com dados relevantes para efeito decisório, responsáveis pelas atividades, cronograma de implementação, compondo o documento denominado “Projeto Executivo” tendo a visibilidade completa do projeto e seus status evolutivos. O documento deve ser entregue para a contratante antes do início da instalação, em até 10 dias úteis a partir do 1º dia útil subsequente a assinatura do contrato. A Diretoria de TI da USCS analisará o documento e dará o aceite em um prazo máximo de 02 dias úteis. Havendo necessidade de adequações a empresa terá um prazo máximo de 02 dias úteis para apresentar o projeto readequado, que será reavaliado pela Diretoria de TI para aprovação, em um prazo máximo de 01 dia útil.

2.9.11. Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno das melhores práticas recomendadas pelos fabricantes dos produtos e softwares envolvidos. Tal conhecimento deverá ser evidenciado por meio de certificações, emitidas pelos respectivos fabricantes ou entidades reconhecidas, que comprovem a qualificação técnica dos profissionais responsáveis pela implantação da solução;

2.9.12. As senhas configuradas no ambiente durante a instalação deverão ter requisito mínimo de 08 (oito) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;

2.9.13. Os profissionais técnicos da Contratada quando em serviço na Universidade Municipal de São Caetano do Sul deverão apresentar documento de identificação oficial com foto, previamente comunicados pela empresa e uniformizados;

2.9.14. A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente.

2.10. SISTEMA DE SEGURANÇA CIBERNETICA

2.10.1. Requisitos técnicos da solução de segurança com inteligência artificial para detecção e resposta estendida a incidentes na camada de proteção nos servidores deverá ser totalmente compatível com a estrutura *in cloud*.

2.10.2. A contratação da prestação dos serviços e a disponibilização da ferramenta deverão atender integralmente aos normativos emitidos pelos órgãos fiscalizadores e de controle competentes, em especial ao disposto na Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

2.10.3. A plataforma deve contar com agentes da Inteligência Artificial para auxiliar em toda a etapa da investigação.

2.10.4. A plataforma deve disponibilizar comunicação direta por texto com os agentes da Inteligência Artificial.

2.10.5. A solução deve ser concebida nativamente sobre uma arquitetura distribuída de múltiplos agentes de software autônomos, sendo no mínimo 6 agentes de IA, não podendo ser um mero agregado de ferramentas de terceiros.

2.10.6. Cada agente deve ser um processo de baixo impacto (low footprint) em termos de consumo de CPU e memória, capaz de operar de forma contínua no ativo (servidor, computador, etc.) sem degradar sua performance.

2.10.7. Os agentes de IA utilizaram o seu conhecimento para orquestrar atividade nos ativos, de acordo com a demanda as atividades serão auditadas, executadas e documentadas.

2.10.8. A IA e os seus agentes devem ser o motor de orquestração central, utilizando um modelo de Gráfico de Conhecimento (Knowledge Graph) para mapear dinamicamente e em tempo real os relacionamentos entre todos os ativos do ambiente (identidades, dispositivos, aplicações, dados, vulnerabilidades, etc.) e organizá-los em um contexto de dados no qual os agentes tenham a capacidade de personalizar a interação do usuário, diminuir a complexidade, aumentar a qualidade e a produtividade.

2.10.9. A plataforma deve ser capaz de, a partir da análise deste gráfico, inferir cadeias de ataque (Cyber Kill Chains) complexas e multivetoriais, correlacionando eventos de baixa relevância que, isoladamente, não seriam considerados ameaças.

2.10.10. A resposta a incidentes deve ser dinâmica e contextual, baseada nas inferências do motor cognitivo, superando a execução de fluxos de trabalho estáticos e lineares.

2.10.11. A plataforma deve disponibilizar durante a navegação, interação com a Inteligência Artificial e acesso aos dados investigados.

2.10.12. A plataforma deve utilizar diferentes agentes da Inteligência Artificial para investigação de endpoints, alertas e Inteligência de ameaças.

2.10.13. A inteligência Artificial deve ser capaz de buscar todos os endpoints cadastrados, alertas abertos e vulnerabilidades identificadas na interação por texto e o resultado deve ser retornado em tela.

2.10.14. Os agentes de Inteligência devem ser capazes de correlacionar todos os dados coletados, analisar e fornecer um parecer investigativo sobre quais ações foram e/ou devem ser realizadas.

2.10.15. Deve usar um modelo matemático gerado a partir de aprendizado de máquina para comparar diferentes características de um arquivo executável, de forma estática, para determinar se ele é malicioso.
2.10.16. A plataforma deve ser capaz de detectar vazamentos de dados relacionados à Contratante, indicando o tipo de dado exposto e as datas que ocorreram.
2.10.17. A plataforma através dos agentes da Inteligência Artificial deve ser capaz de reclassificar a pontuação de risco da ameaça de acordo com a técnica explorada e a classificação do ativo;
2.10.18. A plataforma deve ser capaz de se integrar a aplicações e equipamentos da Contratante para enriquecer a detecção e resposta estendida em tempo real;
2.10.19. A proteção deve estar disponível para os sistemas operacionais Windows, Linux e MacOS.
2.10.20. Prevenção de ameaças baseada em comportamento para análise dinâmica de processos em execução.
2.10.21. Prevenção de exploração por técnicas conhecidas de exploits.
2.10.22. Prevenção de exploração baseada em kernel.
2.10.23. Prevenção de ameaças com base em inteligência de ameaças, como hash de arquivos.
2.10.24. Integração automatizada com um serviço de prevenção de malware, baseado em nuvem do próprio fabricante.
2.10.25. A solução deve prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros.
2.10.26. A solução deve ser compatível, no mínimo, com os seguintes sistemas operacionais e distribuições:

- Windows;
- Ubuntu;
- Oracle Linux;
- RedHat.

2.10.27. A solução deve incluir na análise de execução, no mínimo, as seguintes características:

- Táticas e técnicas de acordo com o modelo de ameaças MITRE ATT&CK;
- Caraterísticas comportamentais suspeitas;
- Detalhes do arquivo como nome, hash, tamanho, tipo;
- Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
- Leitura e escrita de arquivos em disco;
- Leitura e alteração de chaves de registro.

2.10.28. Detalhes de processos iniciados durante a execução.
2.10.29. Atualizações transparentes do mecanismo de detecção de ameaças.
2.10.30. Proteção contra malware, ransomware e ataques sem arquivo.
2.10.31. Identificação e prevenção de tentativas de escalonamento de privilégios ao nível de Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux.
2.10.32. Deve permitir gerar alertas das soluções integradas.
2.10.33. Deve permitir a consulta de eventos de forma integrada.
2.10.34. Os usuários locais da solução devem ter uma política de senha que permita, no mínimo as seguintes configurações, alteração no primeiro login e identificação de complexidade de senha.
2.10.35. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless).
2.10.36. No caso de detecção de um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos.
2.10.37. A solução deve disponibilizar o rastreio de detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências.
2.10.38. A solução deve disponibilizar o rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante.
2.10.39. A solução deve disponibilizar o rastreio de tentativas de roubo de credenciais e\ou tentativa de acessos indevidos a recursos chave do sistema operacional.
2.10.40. Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa artefatos, destacando rapidamente índices de comprometimento já conhecidos.
2.10.41. Gerenciamento unificado e centralizado de todas as funções na mesma console de, bem como a instalação e atualização dos agentes.
2.10.42. A solução deve possuir o recurso de autenticação, por usuário e senha, integrado a sistemas de e-mail, como o do Google (G-Suíte) ou da Microsoft (Office 365) para autenticar utilizando o método SSO (Single Sign On).
2.10.43. Detecção de comprometimento: vírus, malware, backdoors, hosts em comunicação com sistemas infectados por botnet, serviços da Web vinculados a conteúdo malicioso.
2.10.44. Frequência de atualização, personalizável por dia, semana ou mês.
2.10.45. Varredura em tempo real de arquivos (gravação, renomeio e leitura) e de processos em memória.
2.10.46. Monitoramento em tempo real para captura de malwares que são executados em memória sem a necessidade de escrever em arquivo.
2.10.47. Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise comportamental, realizado por inteligência artificial.
2.10.48. Solução única para proteção contra malwares e ransomware, com a capacidade de coletar dados de sistemas operacionais e de rede para detecção de eventos maliciosos, sem a obrigatoriedade de criação e ativação de regras manualmente.
2.10.49. A solução deve permitir instalação silenciosa do agente, em sistemas operacionais Windows, através de pacotes MSI e executável EXE.
2.10.50. A solução deverá ser capaz também de analisar ameaças, sem o uso de assinaturas, fazendo esta análise por comportamento.

2.10.51. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações.
2.10.52. A solução deve suportar nativamente a integração com terceiros, sem a necessidade de instalação de recursos adicionais para receber eventos de múltiplas fontes de origem.
2.10.53. A solução deve disponibilizar, informações sobre o número de dispositivos que possuem o agente instalado e a versão do agente.
2.10.54. A solução deve ser capaz de monitorar e-mail e domínio para identificar vazamento de dados.
2.10.55. Requisitos de detecção e resposta do agente
2.10.56. A solução não deve ter limitação para recebimento de eventos.
2.10.57. A comunicação entre agente e plataforma deve acontecer através do protocolo TCP porta 443;
2.10.58. O agente deve permitir a sua instalação em sistema operacional Linux Ubuntu 24.04 ou superiores.
2.10.59. A solução deve utilizar criptografia para conexão entre agente e plataforma, no mínimo, TLS 1.3 com AES 256.
2.10.60. A solução deve utilizar criptografia nos dados enviados para a plataforma de gerenciamento, no mínimo, AES 256.
2.10.61. A solução deve utilizar algoritmos de aprendizado de máquina para identificar padrões e comportamentos suspeitos.
2.10.62. A solução deverá ser capaz de bloquear tanto ameaças conhecidas como também as desconhecidas.
2.10.63. O agente deve detectar e proteger o dispositivo mesmo offline.
2.10.64. O agente deve receber atualizações de forma automática.
2.10.65. O agente deve receber as novas assinaturas de segurança em tempo real.
2.10.66. A solução deve utilizar detecção de ameaças por meio de dados e padrões baseados em comportamentos, que se utilizam de motores baseados em aprendizado de máquina para averiguação de arquivos.
2.10.67. O agente deve possuir a funcionalidade de inteligência contra malware.
2.10.68. O agente deve possuir a funcionalidade de inteligência contra ransomware.
2.10.69. O agente deve possuir a funcionalidade de bloqueio de indicadores de comprometimento.
2.10.70. O agente deve disponibilizar na sua interface, os seguintes dados:
2.10.70.1. Nome do usuário logado;
2.10.70.2. Nome do host;
2.10.70.3. Informações de sistema operacional (Build, Plataforma);
2.10.70.4. Estado do equipamento (Online ou Offline);
2.10.70.5. Última data comunicação com a console de gerenciamento;
2.10.70.6. Informações relacionadas à rede (IP, DNS, DHCP).
2.10.71. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela contratada.
2.10.72. A solução deve operar em tempo real, monitorando e bloqueando as ameaças.
2.10.73. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes.
2.10.74. A solução deve fornecer a capacidade de executar análises de estações de trabalho/servidores sem a necessidade de interagir com o usuário. Essa capacidade deve ser centralizada e transparente para o usuário.
2.10.75. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger e atualizar.
2.10.76. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho.
2.10.77. A solução deve ser capaz de fazer análise avançada e utilizar algoritmos de aprendizado de máquina, mesmo que sem conexão ao servidor de gerenciamento.
2.10.78. Consulta APIs: Capacidade de extrair dados de segurança e eventos para integração, utilizando os protocolos SSH, HTTP, SNMP e Syslog em todos os itens fornecidos dentro da solução proposta.
2.10.79. A solução deve disponibilizar um agente instalável e compatível com sistemas operacional, Windows, Linux e MacOS. Com a capacidade de detectar, coletar e enviar a plataforma, comportamentos maliciosos de aplicações que estão sendo executadas no sistema operacional.
2.10.80. A solução deve disponibilizar um coletor com capacidade de executar consultas de coleta de eventos e detecção de ação maliciosas em suas integrações, mesmo se houver indisponibilidade de conectividade.
2.10.81. Atualizações regulares e automáticas de binários e base de dados de segurança.
2.10.82. O agente deve ser compatível com o sistema operacional Linux Ubuntu 24.04 ou superiores.
2.10.83. A solução deve suportar a integração baseada em agente e autenticação.
2.10.84. A solução deve permitir o recebimento de eventos por múltiplos coletores.
2.10.85. A solução deve identificar os eventos por integração e agente.
2.10.86. A solução deve permitir a classificação de severidade, quando cadastrado o dispositivo.
2.10.87. Quanto ao armazenamento
2.10.87.1. A solução deve prover no mínimo 2TB de armazenamento para retenção dos eventos coletados e normalizados pela solução, sem custo adicional ou necessidade de fornecimento de hardware para armazenamento pela Contratante.
2.10.87.2. O evento armazenado pela solução, bem como hardware necessário para tal, é de responsabilidade da empresa Contratada em armazenar em Datacenter.
2.10.87.3. Solução deve ter a capacidade de permitir que a Universidade USCS modifique o período de armazenamento de eventos de Windows, Linux e Firewall de forma independente e através de plataforma gráfica disponibilizada pela solução proposta pela empresa Contratada.
2.10.88. Quanto a Relatórios e Dashboards
2.10.88.1. Visualização de Dados.
2.10.88.2. Painéis de controle para visualização em tempo real de incidentes e status de segurança;
2.10.88.3. Relatórios de incidentes, tendências de segurança e desempenho do sistema, exportando em formatos pdf, csv e html;
2.10.88.4. A solução deve ter capacidade de enviar relatórios através dos protocolos SMTP, HTTP, SFTP e ter integração com soluções de colaboração.

2.11. MONITORAMENTO

2.11.1. O serviço de monitoramento deverá ser composto de tecnologia que seja totalmente apartada do ambiente computacional e de servidores da Universidade Municipal de São Caetano do Sul.

2.11.2. A empresa Contratada deverá monitorar o ambiente 24x7 (vinte e quatro horas por dia, sete dias por semana), conforme descrito nesse documento.

2.11.3. O monitoramento deverá ter vigência de 24 (vinte e quatro) meses.

2.11.4. A disponibilidade e monitoramento deverá ocorrer por 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

2.11.5. Deverá ter **SLA** de disponibilidade da console de gerenciamento de no mínimo **99,982%.**

2.11.6. A solução de monitoramento deverá estar hospedada em Datacenter com a classificação mínima de **Tier II.**;

2.11.7. A solução de monitoramento deverá ter portal de acesso de visualização WEB disponibilizada para a Diretoria de Tecnologia da Informação da Universidade USCS.

2.11.8. Deverá ser capaz de enviar alertas de alteração de status de sensores através de correio eletrônico.

2.11.9. Possuir pelo menos os seguintes status para os sensores de monitoramento: Estado normal, estado de alerta e estado de erro.

2.11.10. Possuir a possibilidade para criação de interface WEB com mapa de distribuição de arquitetura com o monitoramento, podendo ter acesso público e/ou autenticado através de contas de usuários internas da solução de monitoramento.

2.11.11. O monitoramento deverá ser compatível com os principais serviços de nuvem pública.

2.11.12. O sistema de monitoramento deverá contar com aplicativo de administração instalável e homologado para o sistema operacional Linux.

2.11.13. A solução de monitoramento deverá abrir chamado de maneira automática junto a Universidade USCS, após a alteração de um sensor para o estado de alerta ou erro.

2.11.14. A ferramenta de monitoramento deve ser capaz de realizar a coleta de dados de diversos dispositivos e sistemas, incluindo servidores, dispositivos de rede e aplicações. Os principais requisitos incluem:

2.11.15. A ferramenta deverá realizar coleta de métricas de desempenho, como uso de CPU, memória, espaço em disco, latência de rede, e status de serviços. A coleta será feita de forma agendada ou por meio de eventos de trap (alerta gerado pelo próprio dispositivo) onde será necessário que os dispositivos entreguem as informações através do protocolo SNMP.

2.11.16. A ferramenta deverá ser capaz de monitorar diversos tipos de hosts, com a possibilidade de utilização de agentes para coleta de dados, bem como monitoramento sem agentes para dispositivos de rede e outros dispositivos que não possuam um agente instalado.

2.11.17. A ferramenta deve ser capaz de gerar alertas e notificações de forma automatizada, baseados em eventos ou métricas predefinidas. As notificações poderão ser enviadas por e-mail ou outras integrações, como sistemas de gerenciamento de incidentes. A ferramenta deverá também permitir a definição de escalonamentos de alertas e ações automáticas, como reiniciar um serviço ou executar comandos específicos em resposta a incidentes quando houver a disponibilidade de conexão via SSH.

2.11.18. A ferramenta deverá possuir uma interface gráfica baseada na web que permita a visualização de dados em tempo real, com dashboards personalizáveis. A interface deve ser intuitiva, acessível e permitir a criação de relatórios gerenciais com informações detalhadas sobre a saúde e o desempenho da infraestrutura.

2.11.19. A plataforma deverá garantir segurança através de autenticação de usuários e controle de permissões, permitindo a definição de diferentes níveis de acesso. A comunicação entre a ferramenta e os dispositivos monitorados deverá ser criptografada para garantir a proteção dos dados durante a transmissão.

2.11.20. A solução deverá ser escalável, permitindo seu uso tanto em ambientes de pequeno porte quanto em grandes infraestruturas corporativas, com a possibilidade de monitoramento de milhares de dispositivos simultaneamente. Para grandes ambientes, deverá ser possível utilizar proxies para distribuição do monitoramento.

2.11.21. A ferramenta deve permitir a geração de relatórios periódicos, tais como dia anterior, semana anterior, mês anterior, ano anterior e a realização de análises de tendências para prever possíveis falhas ou pontos de saturação da infraestrutura. A análise histórica deverá ser capaz de identificar padrões e comportamentos anormais através do armazenamento dos históricos no recurso tecnológico que a Contratada deverá entregar com o serviço de monitoramento.

2.11.22. A ferramenta deve ser compatível com sistemas operacionais Linux e Windows, e permitir a instalação em ambientes físicos ou virtuais, de acordo com a necessidade do cliente.

2.11.23. A ferramenta deverá utilizar uma base de dados para armazenar as informações coletadas, com a possibilidade de utilização de bancos de dados open-source, como MySQL, PostgreSQL ou similares.

2.11.24. A solução deverá permitir integrações com outras plataformas de TI, como sistemas de gerenciamento de incidentes, plataformas de visualização de dados, e outras ferramentas de automação e análise de infraestrutura.

2.11.25. A implementação da ferramenta será realizada em etapas, incluindo a instalação do proxy através do recurso tecnológico, configuração e personalização conforme os requisitos específicos da infraestrutura de TI.

2.11.26. Deverá ser possível geração de relatórios c/ dados de tabela e gráficos para quaisquer sensores que compõem a solução;

2.12. RELÁTORIOS

2.12.1. Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, contendo:

2.12.2. Relatório de Chamados (referente ao serviço descrito nesse lote).

2.12.3. Categoria do chamado.

2.12.4. Usuário.

2.12.5. Ativos relacionados.

2.12.6. Data de abertura e fechamento.

2.12.7. Status.

2.12.8. Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote).

2.12.9. Disponibilidade.

2.12.10. Consumo de hardware (CPU, memória, disco, consumo de banda).

2.12.11. Alertas e erros.

2.13. SUPORTE TÉCNICO

2.13.1. Os serviços de suporte técnico especializado, deverão contemplar toda a solução e infraestrutura de segurança contidas neste Termo de Referência.

2.13.2. A Contratada deverá administrar e monitorar o serviço de segurança descrito nesse documento;

2.13.3. A USCS poderá abrir chamados de manutenção através de chamada telefônica para número com DDD (11), central de atendimento via navegador (WEB) e correio eletrônico sem a necessidade prévia consulta e/ou qualquer liberação por parte da Contratada.

2.13.4. O atendimento técnico remoto deverá ocorrer 24 horas por dia.

2.13.5. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas de hardware e/ou software.

2.13.6. Toda falha e indisponibilidade no ambiente ocasionado por falhas físicas nos equipamentos (hardware) será de plena responsabilidade da empresa Contratada.

2.13.7. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos.

2.13.8. Será de responsabilidade da Contratada manter o pleno funcionamento das políticas de segurança da solução.

2.13.9. Deverá monitorar diariamente, os relatórios de segurança gerados ao concluir as tarefas, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da Contratada efetuar correção ou ajuste técnico para a normalização dele, garantindo o pleno funcionamento da solução;

2.13.10. A empresa Contratada deverá ser responsável por executar as restaurações do ambiente.

2.13.11. A empresa Contratada se responsabilizará pelas despesas com material de escritório, reprodução de documentos (cópias, etc.) e materiais diversos, que forem necessários à execução dos serviços de manutenção dos serviços e pelos seus profissionais;

2.13.12. A Contratada deverá realizar atendimentos remotos à equipe de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul, a partir de solicitações recebidas dos técnicos ou do gestor do instrumento de contrato a ser celebrado com a empresa vencedora do certame, via sistema de atendimento, telefone ou correio eletrônico;

2.13.13. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados;

2.13.14. Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências;

2.13.15. Manter o ambiente de segurança sempre atualizado em com as melhores práticas aplicadas;

2.13.16. A Contratada deverá garantir que os profissionais designados para atendimento técnico serão capacitados;

2.13.17. A garantia de tempo de resposta será realizada conforme critérios de prioridades elencados no quadro imediatamente abaixo:

Classe	Descrição	Início do Atendimento em até
1	Serviço indisponível	1 hora
2	Suporte técnico de maior impacto	4 horas
3	Suporte técnico com menor impacto	8 horas
4	Manutenção preventiva	Programada

2.13.18. O acordo de nível de serviço **(SLA)** para suporte técnico deverá obedecer ao seguinte escopo:

PRIORIDADE	DESCRIÇÃO
1 (Emergencial)	O serviço está fora de operação ou há um impacto crítico nas operações.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações que sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

2.13.19. As horas para primeiro atendimento e resolução de incidentes são horas corridas e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

2.13.20. Caso seja identificado que o Serviço de Segurança se encontra indisponível por causa de soluções de terceiros, link de internet, indisponibilidade de switch, energia elétrica, roteadores, firewall, problemas de hardware/infraestrutura de TI ou qualquer serviço que interligue as unidades, será de responsabilidade da Contratada em realizar a detecção e resolução do problema.

2.13.21. A empresa Contratada deverá disponibilizar e gerenciar os atendimentos técnicos da Universidade USCS através de portal de gerenciamento de atendimentos com acesso a partir de navegador web;

2.13.22. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central;

2.13.23. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;

2.13.24. A Contratada deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento;

2.13.25. A Contratante deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail;

2.13.26. O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da empresa Contratada, sendo essa responsável por sua atualização e manutenção;

2.13.27. A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;
2.13.28. O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;
2.13.29. A Contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela Contratante;
2.13.30. Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;
2.13.31. Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a Universidade USCS;
2.13.32. O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a Universidade;
2.13.33. Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;
2.13.34. A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";
2.13.35. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;
2.13.36. Deverá ser possível a criação de grupos de usuários na solução;
2.13.37. A solução a ser disponibilizada pela empresa Contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.
2.13.38. Relatórios Mensais, durante o período do contrato;
2.13.39. Relatório de Chamados;
2.13.40. Categoria do chamado;
2.13.41. Usuário;
2.13.42. Ativos relacionados;
2.13.43. Data de abertura e fechamento;
2.13.44. Status;
2.13.45. O suporte técnico deverá ter os seguintes canais de atendimento: Suporte telefônico, e-mail e sistema online de chamados, todos em português do Brasil.
2.13.46. A empresa Contratada deverá sempre disponibilizar versões mais recentes dos softwares sem ônus financeiro.

2.14. MANUTENÇÃO PREVENTIVA DA SOLUÇÃO CIBERNETICA

2.14.1. A manutenção preventiva será destinada a atualizar os componentes de software (atualização tecnológica), conforme definições nesse documento, e a realizar quaisquer operações que evitem uma parada total ou parcial da solução.
2.14.2. A USCS, através de sua equipe técnica de Tecnologia da Informação, observará o desempenho do sistema contratado e, caso necessário, solicitará à Contratada a manutenção preventiva para viabilizar o melhor desempenho da solução.
2.14.3. A manutenção preventiva está inclusa no suporte técnico da solução, sendo prestada pela Contratada sem qualquer ônus adicional para a Universidade.
2.14.4. Durante a manutenção preventiva, a USCS deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta.
2.14.5. Durante o período de suporte técnico deverá ser realizada a atualização de qualquer outro software constituinte da solução para as versões mais recentes, sem ônus adicional imputado à Contratante.
2.14.6. A manutenção corretiva será destinada a remover erros ou falhas apresentadas pelos componentes de software da solução contratada.
2.14.7. Como erro ou falha entende-se a geração de resultado diferente do previsto. Para a resolução desses erros, é necessária a intervenção técnica especializada ou mesmo até a substituição de seus componentes por parte da Contratada.
2.14.8. A manutenção corretiva após o diagnóstico (determinação da origem da falha) deverá ser realizada por meio de ajustes, consertos ou substituição dos elementos que apresentam problemas, restabelecendo a solução suas condições normais de funcionamento ou operação, conforme as especificações do fabricante.
2.14.9. Entende-se como diagnóstico à compilação e análise de informações para definição da causa de um problema.
2.14.10. Entende-se como Recuperação da Disponibilidade a execução de atividades que permitem restabelecer o funcionamento da solução.
2.14.11. A comprovação de isenção de responsabilidade se dará pela apresentação de relatório técnico circunstanciado dos elementos da solução contratada, e pelas demais informações consideradas necessárias pela Contratada para embasar a justificativa.
2.14.12. Tomar todas as providências necessárias para que seus funcionários, representantes e/ou contratados observem os regulamentos, normas e instruções de segurança da informação e Comunicações pela Contratante, quando estiverem executando serviços.
2.14.13. A Contratada deve comprometer-se a manter informações confidenciais no mais estrito sigilo sobre todos os dados, configurações, processos, fórmulas, rotinas e quaisquer outros objetos que sejam disponibilizados, pela USCS à empresa Contratada, para a realização dos trabalhos. Compromete-se a não copiar, não usar em seu próprio benefício, nem revelar ou mostrar a terceiros, nem divulgar tais informações, no território brasileiro ou no exterior, sob pena prevista em lei. Só os representantes e prepostos, devidamente autorizados entre as partes, cuja avaliação das informações confidenciais seja necessária e apropriada, para os propósitos especificados em contrato, terão acesso às mesmas.
2.14.14. Prestar os esclarecimentos necessários para a Contratante, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.
2.14.15. Requisitos sociais, ambientais e culturais
2.14.16. Sistema e todos os seus módulos deve ser desenvolvido/disponibilizado de forma compatível para as características do Brasil quanto a aspectos de interface gráfica, linguagem, legislação, costumes, apresentação, funcionalidades, telas e relatórios. Deve também possuir manuais de usuário on-line, com possibilidade de impressão, e documentação técnica do software em idioma português do Brasil ou inglês.

Anexo II do Contrato ____/2026

Quadro contendo relação de equipamentos físicos as a service, serviços, quantitativos e preços.

LOTE 01 - Serviço de Segurança de Rede - Firewall *As a Service*							
Item	**Solução**	**Fabricante**	**Descrição**	**Modelo /Tipo**	**Cron. Pag.**	**Valor Unitário (em reais)**	**Valor Total (em reais)**
1	*Solução de Firewall as a Service do **tipo 02.***		*Fornecimento de 2 Firewalls de próxima geração em **1 (uma)** estrutura em alta disponibilidade sendo equipamentos configurados no formato **ativo/ativo** com inspeção profunda de pacotes, prevenção contra intrusões, filtragem de conteúdo, controle de aplicações, VPN segura, proteção contra malware e gerenciamento centralizado pelo período de **24 (vinte e quatro)** meses.*		*24 meses*		
2	*Solução de Firewall as a Service do **tipo 01**.*		*Fornecimento de 4 Firewalls de próxima geração distribuídos em **2 (duas)** estruturas em alta disponibilidade sendo equipamentos configurados no formato **ativo/ativo** com inspeção profunda de pacotes, prevenção contra intrusões, filtragem de conteúdo, controle de aplicações, VPN segura, proteção contra malware e gerenciamento centralizado pelo período de **24 (vinte e quatro)** meses.*		*24 meses.*		
3	*Solução de Firewall as a Service do **tipo 03.***		*Fornecimento de 6 Firewalls de próxima geração distribuídos em **3 (três)** estruturas em alta disponibilidade sendo equipamentos configurados no formato **ativo/ativo** com inspeção profunda de pacotes, prevenção contra intrusões, filtragem de conteúdo, controle de aplicações, VPN segura, proteção contra malware e gerenciamento centralizado pelo período de **24 (vinte e quatro)** meses.*		*24 meses*		
4	*Serviço especializado em suporte técnico com atendimento local e remoto nos serviços de Next Generation firewall dos **tipos 1, 2 e 3.***	Não preencher	*Serviço de Suporte Técnico com Atendimento Local e Remoto para os equipamentos de next Generation firewall em conformidade com as especificações contidas no termo de referência.*	Serviço	*24 meses*		
5	*Serviço especializado em monitoramento com atendimento para os serviços de Next Generation firewall dos **tipos 1, 2 e 3.***	Não preencher	*Serviço de Monitoramento (Noc) para os equipamentos de next Generation firewall em conformidade com as especificações contidas no termo de referência.*	Serviço	*24 meses*		
6	*Serviço especializado em instalação do Next Generation firewall dos **tipos 1, 2 e 3.***	Não preencher	*Serviço de instalação, configuração de todas as funções do serviço de next Generation firewall e criação da documentação final do projeto incluindo:* • *Planejamento e Projeto Executivo;* • *Instalação Física;* • *Configuração Lógica e Alta Disponibilidade;*	Serviço	*01*		

			• *"As built" (diagramas, parâmetros, endereçamentos, políticas);* • *Relatórios de testes (pré/pós) e Termo de Aceite.*				
Valor Global do Lote Contratado (em reais)							

LOTE 02 – Serviço de Hospedagem em nuvem Privada para a Estrutura Computacional USCS – Data Center Hosting							
Item	**Solução**	**Fabricante**	**Descrição**	**Modelo /Tipo**	**Cron. Pag.**	**Valor Unitário (em reais)**	**Valor Total (em reais)**
1	*Serviço de instalação configuração e documentação total do ambiente **em nuvem.***	Não preencher	*Serviço de Instalação e Configuração de toda a infraestrutura em nuvem, incluindo:* • *Planejamento e Projeto Executivo;* • *Provisionamento do ambiente de virtualização;* • *Conectividade e segurança;* • *Migração do ambiente;* • *Segurança, conformidade e controles operacionais;* • *Documentação as built + inventário lógico do ambiente;* • *Relatórios de atualização/compatibilidade e de testes (pré/pós-migração) e Termo de Aceite.*	*Serviço*	*01*		
2	*Serviço especializado de **hosting** para suportar o ambiente computacional.*	Não preencher	*Serviço de Data Center Hosting com infraestrutura redundante, alta disponibilidade, climatização controlada, segurança física e lógica, conectividade de alta performance.*	*Serviço*	*24 meses*		
3	*Serviço especializado de suporte técnico no ambiente computacional **em nuvem**.*	Não preencher	*Serviço de Suporte Técnico com Atendimento Remoto para a infraestrutura em nuvem.*	*Serviço*	*24 meses*		
4	*Serviço especializado de monitoramento no ambiente computacional **em nuvem.***	Não preencher	*Serviço de Serviço de Monitoramento (NOC) remoto para a infraestrutura em nuvem.*	*Serviço*	*24 meses*		
Valor Global do Lote Contratado (em reais)							

Valor Global do Contrato (em reais)	

ANEXO XIV

ANEXO LC-01 - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO
(Contratos)

Contratante: Universidade Municipal de São Caetano do Sul

Contratada: _____

Contrato nº (de origem):_____

OBJETO: Contratação de empresa especializada para o fornecimento de infraestrutura e serviços de hospedagem em nuvem, bem como solução de segurança perimetral (Next Generation Firewall) para atendimento ao ambiente de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul - USCS, conforme condições e especificações constantes no Termo de Referência do Edital.

Advogado (S)/ nº OAB: (*)_____

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, conforme dados abaixo indicados, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais do responsável pela contratante estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no artigo 2º da Instrução nº 01/2020, conforme "Declaração de Atualização Cadastral" anexa;

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados..

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

São Caetano do Sul, ___de _____de 2026.

Autoridade Máxima da Universidade Municipal de São Caetano do Sul.

Nome: _____

Cargo: _____

CPF: _____

Responsável pela Homologação e adjudicação do Certame.

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Responsáveis que assinam o instrumento Contratual

Pela USCS

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Pela Contratada

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Ordenador de Despesas da Universidade Municipal de São Caetano do Sul

Nome: _____

Cargo: _____

CPF: _____

Assinatura:_____

Agentes públicos responsáveis pela gestão do instrumento contratual

Gestor do Contrato

Nome: _____

Cargo: _____

CPF: _____

Assinatura: _____

Fiscalizador técnico do Contrato

Nome: _____

Cargo: _____

CPF: _____

Assinatura: _____

Demais Responsáveis (**):
Tipo de ato sob sua responsabilidade:
Nome:_____
Cargo:_____
CPF:_____
Assinatura:_____

Advogado
(*). Facultativo, indicar quando já constituído, informando, inclusive, o endereço eletrônico.

(**) - O Termo de Ciência e Notificação e/ou Cadastro do(s) Responsável(is) deve identificar as pessoas físicas que tenham concorrido para a prática do ato jurídico, na condição de ordenador da despesa; de partes contratantes; de responsáveis por ações de acompanhamento, monitoramento e avaliação; de responsáveis por processos licitatórios; de responsáveis por prestações de contas; de responsáveis com atribuições previstas em atos legais ou administrativos e de interessados relacionados a processos de competência deste Tribunal. Na hipótese de prestações de contas, caso o signatário do parecer conclusivo seja distinto daqueles já arrolados como subscritores do Termo de Ciência e Notificação, será ele objeto de notificação específica. (inciso acrescido pela Resolução nº 11/2021).

ANEXO LC-02 - DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TCE-SP

CONTRATANTE: UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL

CNPJ Nº: 44.392.215/0001-70

CONTRATADA:

CNPJ Nº:

CONTRATO N° ____/2026

DATA DA ASSINATURA: ___/__/2026

VIGÊNCIA: 24 meses.

OBJETO: Contratação de empresa especializada para o fornecimento de infraestrutura e serviços de hospedagem em nuvem, bem como solução de segurança perimetral (Next Generation Firewall) para atendimento ao ambiente de Tecnologia da Informação da Universidade Municipal de São Caetano do Sul - USCS, conforme condições e especificações constantes no Termo de Referência do Edital.

Valor global R$ _____ (_____).

Declaro, na qualidade de responsável pela entidade supra epigrafada, sob as penas da Lei, que os demais documentos originais, atinentes à correspondente licitação, encontram-se no respectivo processo administrativo arquivado na origem à disposição do Tribunal de Contas do Estado de São Paulo, e serão remetidos quando requisitados.

São Caetano do Sul, ___ de _____ de 2026.

_____

Prof. Dr. Leandro Campi Prearo – Reitor

Universidade Municipal de São Caetano do Sul - USCS

leandro.prearo@online.uscs.edu.br

ANEXO PC-02 - CADASTRO DO RESPONSÁVEL

Entidade: UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL

Nome:

Cargo:

CPF:

Período de gestão: 01 de março de 2025 a 28 de fevereiro de 2029.

Obs: 1. Todos os campos são de preenchimento obrigatório.

2. Repetir o quadro, se necessário, informando todos os responsáveis durante o exercício.

3. Anexar a “Declaração de Atualização Cadastral” emitida pelo sistema

“Cadastro Corporativo TCESP – CadTCESP”, por ocasião da remessa do presente documento ao TCESP”.

As informações pessoais dos responsáveis estão cadastradas no módulo eletrônico do Cadastro TCESP, conforme previsto no Artigo 2º das Instruções nº01/2020, conforme “Declaração de Atualização Cadastral” ora anexada (s).

_____

Nome e assinatura do responsável pelo preenchimento

ANEXO XV
ESTUDO TÉCNICO PRELIMINAR

FUNDAMENTAÇÃO

Atualmente a estrutura da Universidade de São Caetano do Sul, vem apresentando a necessidade de crescimento dos recursos computacionais a serem aportados principalmente para a equipe de desenvolvimento interna da universidade.
A idealização de um cenário de servidores em nuvem é extremamente importante para o bom desenvolvimento e saúde dos projetos que são e os demais que serão executados pela equipe interna.

A adoção de servidores em nuvem pela universidade oferece uma série de benefícios estratégicos, especialmente no que diz respeito à segurança, alta disponibilidade e escalabilidade. Ao hospedar os servidores em nuvem, a universidade pode garantir uma infraestrutura mais resiliente e protegida contra ameaças externas. Nesse ambiente de nuvem há oferta de segurança robusta, com mecanismos de proteção como criptografia de dados, monitoramento contínuo e práticas de controle de acesso avançadas, o que torna mais difícil a ocorrência de falhas de segurança. Além disso, muitos provedores de serviços em nuvem adotam políticas de segurança de nível corporativo, com protocolos de defesa contínuos e auditorias periódicas.

A alta disponibilidade é outro ponto fundamental que a nuvem proporciona. Com a distribuição geográfica dos servidores e a redundância de infraestrutura, os sistemas da universidade permanecem operacionais mesmo em caso de falhas em alguns componentes. A nuvem permite que os recursos sejam realocados automaticamente, garantindo que os serviços estejam sempre disponíveis, sem interrupções significativas. Isso é essencial para o funcionamento contínuo dos serviços acadêmicos e administrativos, que não podem sofrer paradas prolongadas.

Além disso, a escalabilidade que a nuvem oferece é um dos seus maiores atrativos. A universidade pode aumentar ou diminuir sua capacidade de processamento e armazenamento de forma dinâmica, conforme a demanda. Isso é especialmente importante durante períodos de maior uso, como no início de semestres ou em eventos acadêmicos, garantindo que o ambiente digital da universidade seja sempre capaz de atender a um número variável de usuários, sem comprometer o desempenho.

Fora a necessidade dos serviços de nuvem, precisamos atender a necessidade de conectividade, onde todos os equipamentos e subscrições se encontram defasados sendo necessário a aquisição de novos equipamentos de Next Generation Firewall para todos os Campi:

UNIVERSIDADE SÃO CAETANO DO SUL					
CAMPUS BARCELONA Endereço: Av. Goiás, 3400 - Barcelona, São Caetano do Sul - SP, CEP: 09550-051.	CAMPUS CENTRO Endereço: R. Santo Antônio, 50 - Centro, São Caetano do Sul - SP, CEP: 09521-160.	CAMPUS CENTRO 2 Endereço: Rua Samuel Klein, 83 2° Andar - Centro - São Caetano do Sul - CEP: 09510-125.	CAMPUS CONCEIÇÃO Endereço: Rua Conceição, 321 - Santo Antônio - São Caetano do Sul - 09530-060.	CAMPUS ITAPETININGA Endereço: Av. Dr. Ciro Albuquerque, 4750 - Taboãozinho, Itapetininga - SP, CEP: 18200-021.	CAMPUS MANOEL COELHO Endereço: Rua Manoel Coelho, 600 - 6º andar - Centro, São Caetano do Sul - SP, Cep: 09510-101.

No entanto, para garantir uma camada adicional de segurança na nuvem, é fundamental a implementação de um Next Generation Firewall (NGFW) para todos os campis da universidade. Um NGFW vai além das funções tradicionais de filtragem de pacotes e pode identificar e bloquear ameaças avançadas, como malware, ransomware e ataques direcionados. Ele também oferece inspeção profunda de pacotes e integração com sistemas de inteligência de ameaças, tornando-se essencial para proteger o ambiente universitário de ataques cibernéticos sofisticados. Além disso, o NGFW permite a segmentação de redes, facilitando o controle rigoroso sobre quem tem acesso a determinados recursos, o que é crucial para a proteção dos dados sensíveis da instituição e dos usuários. Dessa forma, a combinação de servidores em nuvem com um Next Generation Firewall e uma solução de antivírus com inteligência artificial nativa oferece à universidade uma infraestrutura segura, ágil e capaz de suportar o crescimento contínuo de suas operações acadêmicas e administrativas.

A implementação de uma solução de antivírus é fundamental para garantir a segurança e a integridade dos sistemas da universidade. Com o aumento constante de ameaças cibernéticas, como malwares, vírus, ransomwares e ataques de phishing, a proteção de dados e a prevenção de infecções são essenciais para preservar a operação contínua e a confiança da comunidade acadêmica.

Os sistemas acadêmicos, administrativos e de pesquisa da universidade contêm informações altamente sensíveis, como dados pessoais de estudantes, professores e funcionários, registros acadêmicos, pesquisas e informações financeiras. Se esses dados forem comprometidos, isso pode resultar em prejuízos financeiros, danos à reputação da instituição e até mesmo a perda de informações valiosas. O antivírus oferece uma camada de proteção constante contra esses riscos, monitorando e detectando qualquer comportamento suspeito ou arquivo malicioso antes que ele tenha a chance de causar danos aos sistemas e às redes.

Além disso, as ameaças estão cada vez mais sofisticadas, e um antivírus moderno vai além da simples detecção de vírus conhecidos. As soluções mais avançadas utilizam inteligência artificial e aprendizado de máquina para identificar comportamentos anômalos e prevenir ataques desconhecidos, o que garante uma proteção proativa. A atualização contínua do banco de dados de assinaturas do antivírus também assegura que a instituição esteja sempre protegida contra as últimas ameaças, sem a necessidade de intervenção manual.

Uma solução de antivírus eficaz também contribui para o desempenho geral da rede e dos dispositivos, minimizando o risco de contaminação e evitando a propagação de infecções, o que pode comprometer a produtividade acadêmica e administrativa. Além disso, o antivírus pode ajudar na conformidade com regulamentos de segurança e privacidade, como a Lei Geral de Proteção de Dados (LGPD), ao garantir que os dados pessoais sejam mantidos de maneira segura e protegida contra acessos não autorizados.

RESUMO

Portanto, a implementação de um serviço de servidores em nuvem, Next Generation Firewall e antivírus robusta, e eficiente é essencial para proteger a infraestrutura tecnológica da universidade, garantir a continuidade das atividades acadêmicas e administrativas e mitigar riscos associados à perda de dados, danos à reputação e a compromissos legais.

Acrescem-se a esses aspectos as consequentes vantagens:

- Segurança e Proteção de Dados:
A contratação de Next Generation Firewall (NGFW) e antivírus com inteligência artificial proporciona uma camada robusta de segurança para os ativos digitais da universidade. Esses recursos permitem inspeção profunda de pacotes, identificação e bloqueio de ameaças sofisticadas, prevenção de ataques e conformidade com a Lei Geral de Proteção de Dados (LGPD);

- Alta Disponibilidade e Continuidade dos Serviços:
A hospedagem em nuvem garante alta disponibilidade e realocação automática de recursos, assegurando operação ininterrupta de sistemas críticos, inclusive durante falhas ou picos de demanda.

- Escalabilidade e Flexibilidade:
A solução em nuvem permite ampliação ou redução de recursos conforme a sazonalidade e necessidade da USCS, como em períodos de matrícula, aplicação de provas e eventos institucionais.

- Previsibilidade Orçamentária e Redução de Custos Operacionais:
Ao adotar o modelo "as a service", a USCS evita despesas inesperadas com aquisição, atualização e manutenção de hardware, favorecendo a previsibilidade financeira.

- Cobertura Abrangente e Padronização:
O modelo contempla todos os campi da universidade, assegurando homogeneidade nos padrões de segurança e qualidade do serviço.

INDENTIFICAÇÃO DAS SOLUÇÕES

SERVIÇO DE SEGURANÇA PARA ESTAÇÕES DE TRABALHO, SERVIDORES E PERIMETRO.

	ITEM	DESCRIÇÃO	QTDE
LOTE 01	01	SERVIÇO DE SEGURANÇA FIREWALL AS A SERVICE TIPO 1.	24
	02	SERVIÇO DE SEGURANÇA FIREWALL AS A SERVICE TIPO 2.	24
	03	SERVIÇO DE SEGURANÇA FIREWALL AS A SERVICE TIPO 3.	24
	04	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	01
	05	SERVIÇO DE SUPORTE TÉCNICO COM ATENDIMENTO LOCAL E REMOTO	24
	06	SERVIÇO DE MONITORAMENTO (NOC)	24

SERVIÇO DE DATA CENTER HOSTING.

	ITEM	DESCRIÇÃO	QTDE
LOTE 02	01	SERVIÇO DE DATA CENTER HOSTING.	24
	02	SERVIÇO DE SUPORTE TÉCNICO.	24
	03	SERVIÇO DE MONITORAMENTO (NOC).	24
	04	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	01

OPÇÃO DECONTRATAÇÃO

A contratação deverá ser dividida em dois lotes. O 1º (primeiro) lote será baseado em serviços de segurança, e o 2º (segundo) lote, em serviços de data center em nuvem. Todo o processo será realizado no formato de prestação de serviços. O fornecimento dos serviços deverá abranger toda a demanda necessária para o perfeito funcionamento, incluindo o fornecimento de hardwares, softwares, garantias, serviços de instalação, suporte técnico, monitoramento e segurança. A remuneração será baseada em valor fixo mensal, com avaliação de qualidade e disponibilidade dos serviços prestados, conforme os Acordos de Níveis de Serviço, e com glosas específicas em caso de não cumprimento dos resultados esperados ou de obrigações não entregues.

O modelo respeita os dispositivos da Lei nº 14.133/2021, especialmente quanto à eficiência, transparência, divisão em lotes e adoção de critérios objetivos de medição de desempenho. A divisão em dois lotes (segurança e data center) está adequada aos princípios da segregação de objetos e especialização de fornecedores.

SUMÁRIO DE PREÇOS COLETADOS ATRAVÉS DO PNCP

Esses tipos de contratação foram sumarizados para a análise dos termos de referências das seguintes contratações realizadas e avaliação dos valores investidos:

1. Descrição do serviço similar ao lote 1.

DESCRIÇÃO	
Modalidade	Pregão Eletrônico.
Edital	545085/2020.
Data da Publicação	28/07/2022
Órgão Solicitante	Câmara dos Deputados - Palácio do Congresso Nacional - Praça dos Três Poderes
Valor total	R$ 25.599.875,37
Link	https://www.camara.leg.br/licitacoes-e-contratos/licitacoes/18646
Objeto	Aquisição de solução de rede de comunicação de dados, com equipamentos e acessórios novos e para primeiro uso, incluindo instalação, implantação, capacitação operacional e garantia de funcionamento, pelo período de 60 (sessenta) meses.

2. Descrição do serviço similar ao lote 2.

DESCRIÇÃO	
Modalidade	Pregão Eletrônico.
Edital	4/04/2024
Data da Publicação	20/03/2024
Órgão Solicitante	Prefeitura Municipal de Camalaú.
Valor total	R$ 56.700,00/Mensal
Link	https://pncp.gov.br/app/editais/09073271000141/2024/10
Objeto	Contratação de empresa especializada para fornecer licença de uso particular, de Sistema de Gestão de Saúde Mobile e WEB integrados e em nuvem (SAAS - Software as a Service), no âmbito da Secretaria de Saúde do Município de Camalaú-PB, incluindo os serviços de acompanhamento de resultados e indicadores da Atenção Primária em Saúde segundo a política de financiamento do Ministério da Saúde, Produção dos Agentes Comunitários de Saúde e dos Agentes de Combate às Endemias, bem como a hospedagem em nuvem e backup (Cloud Server) do Sistema da Atenção Básica (e-SUS/PEC) do Ministério da Saúde, para atender as necessidades de informatização da produção da Atenção Básica e da Vigilância em Saúde,

	cumprindo assim com as normas e Portarias Ministeriais, efetivando a integração do sistema de informação e-SUS, e entre demais sistemas do Ministério da Saúde, que possibilite integração, conforme especificações técnicas e quantitativos descritos no termo de referência. Os serviços deverão conter: instalação das Plataforma Tecnológicas, com a preparação dos dispositivos móveis necessários, implantação e suporte técnico dos Sistemas e treinamento dos usuários permitindo maior efetividade no processamento e cumprindo com as normas e Portarias Ministeriais garantindo segurança no envio das informações no padrão do Ministério da Saúde

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Os cenários avaliados foram precificados e analisados individual, financeira e tecnicamente, para identificação de seus benefícios para o ambiente de tecnologia da Universidade de São Caetano do Sul, como também para o estabelecimento de parâmetro em relação ao custo de contratação em prol da otimização do uso dos recursos disponíveis para esta pretensa contratação.

Foi realizada pela Diretoria de Tecnologia da Informação Inovação da USCS, a pesquisa de preços conforme Projeto Básico.

Foram levantadas as condições do mercado para fornecimento dos serviços conforme condições estabelecidas no Processo de Compra 419/2025 que fora **anulado**, respeitando-se os parâmetros da Lei Federal nº 14.133, vigente desde abril de 2021.

*EMPRESA – COTAÇÃO – 1	
Data da solicitação	14/11/2025
Valor Total	R$ 4.323.420,00
Descrição do Lote 1	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE SEGURANÇA SE BASEANDO EM FIREWALL AS A SERVICE, SUPORTE TÉCNICO E MONITORAMENTO 24X7.
Descrição do Lote 2	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE HOSTING, SUPORTE TÉCNICO E MONITORAMENTO 24X7.

*EMPRESA – COTAÇÃO – 2	
Data da solicitação	14/11/2025
Valor Total	R$ 4.334.867,37
Descrição do Lote 1	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE SEGURANÇA SE BASEANDO EM FIREWALL AS A SERVICE, SUPORTE TÉCNICO E MONITORAMENTO 24X7.
Descrição do Lote 2	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE HOSTING, SUPORTE TÉCNICO E MONITORAMENTO 24X7.

*EMPRESA – COTAÇÃO – 3	
Data da solicitação	17/11/2025
Valor Total	R$ 4.211.835,65
Descrição do Lote 1	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE SEGURANÇA SE BASEANDO EM FIREWALL AS A SERVICE, SUPORTE TÉCNICO E MONITORAMENTO 24X7.
Descrição do Lote 2	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE HOSTING, SUPORTE TÉCNICO E MONITORAMENTO 24X7.

*EMPRESA – COTAÇÃO – 4	
Data da solicitação	14/11/2025
Valor Total	R$ 4.241.601,00
Descrição do Lote 1	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE SEGURANÇA SE BASEANDO EM FIREWALL AS A SERVICE, SUPORTE TÉCNICO E MONITORAMENTO 24X7.
Descrição do Lote 2	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE HOSTING, SUPORTE TÉCNICO E MONITORAMENTO 24X7.

*EMPRESA – COTAÇÃO – 5	
Data da solicitação	17/11/2025
Valor Total	R$ 4.202.100,00
Descrição do Lote 1	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE SEGURANÇA SE BASEANDO EM FIREWALL AS A SERVICE, SUPORTE TÉCNICO E MONITORAMENTO 24X7.
Descrição do Lote 2	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA SERVIÇO DE HOSTING, SUPORTE TÉCNICO E MONITORAMENTO 24X7.

*****A razão social e o número do CNPJ da empresa estão disponíveis para consulta física no vol. 01 do processo de compras 848/2025

Baseado nessas consultas obtivemos o orçamento inicial estimado para contratação no valor de R$ 4.316.670,05 (quatro milhões, trezentos e dezesseis mil, seiscentos e sertenta reais e cinco centavos) considerando o fornecimento de hardware, software, garantia e serviços por prazo de 24 (vinte e quatro) meses.

A pesquisa de mercado, com base em contratos similares no Portal Nacional de Contratações Públicas (PNCP), demonstrou compatibilidade de preços e confirma que os valores estimados estão dentro da média de mercado, assegurando a economicidade da contratação.

CONSIDERAÇÕES FINAIS

Para o completo funcionamento do ambiente de tecnologia da universidade, é essencial a implementação de soluções robustas e atualizadas, como o Next Generation Firewall, a solução de antivírus e os serviços de data center em cloud. O Next Generation Firewall oferece uma proteção avançada contra ameaças cibernéticas, garantindo a segurança das redes e dos dados sensíveis.

Já a solução de antivírus é fundamental para proteger os dispositivos e sistemas contra malwares e ataques virtuais, evitando riscos que possam comprometer a integridade das informações. Além disso, o serviço de data center em cloud proporciona escalabilidade, flexibilidade e alta disponibilidade, permitindo o armazenamento e processamento de grandes volumes de dados com eficiência e sem interrupções. Juntas, essas tecnologias formam a espinha dorsal da infraestrutura de TI da universidade, assegurando a continuidade dos serviços e o desenvolvimento de um ambiente acadêmico seguro e inovador.

Diante do exposto, o entendimento desta Diretoria é que o modelo de contratação proposto é vantajoso, tecnicamente adequado, econômico e viável, sendo essencial para garantir a continuidade das atividades institucionais, a segurança dos dados e a modernização da infraestrutura de Tecnologia da Informação da USCS.

APROVAÇÃO E ASSINATURA

_____

Alessandro Parada

Diretor de Tecnologia da Informação e Inovação

ANEXO XVI
PLANO DE GESTÃO DE RISCO

INFRAESTRUTURA E SEGURANÇA DE REDE E SERVIÇO DE HOSPEDAGEM EM NUVEM PRIVADA – DATA CENTER

1. INTRODUÇÃO

Este Plano de Gestão de Riscos foi elaborado com base no Estudo Técnico Preliminar (ETP) para a contratação dos serviços de segurança de rede (Lote 01) e serviços de data center em nuvem privada cloud computing (Lote 02).

Em conformidade com o artigo 6º, inciso XXVII da Lei nº 14.133/2021, este documento tem por finalidade identificar, avaliar, tratar e monitorar os eventuais riscos que possam comprometer a execução contratual e a continuidade dos serviços essenciais para o ambiente tecnológico da Universidade Municipal de São Caetano do Sul.

A gestão de riscos é essencial para aumentar a capacidade de lidar com incertezas, estimular a transparência, contribuir para o uso eficiente de recursos e melhorar a entrega de serviços. Este documento pressupõe orientar as atividades relacionadas ao projeto de contratação dos serviços firewall *as a service* e alocação do parque computacional a partir da migração das aplicações baseado em infraestrutura tecnológica em nuvem, ancorado no conceito de alta disponibilidade, com oferta de serviço especializado de instalação, gerenciamento, suporte técnico avançado e monitoramento constante no formato 24x7, de forma a prever eventos que possam comprometer os objetivos do projeto.

2. OBJETIVO

O plano tem como objetivo orientar a gestão de riscos desde o início do projeto até a sua conclusão, fornecendo uma abordagem para identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos associados ao projeto de serviços de segurança e data center.

Assegurar a continuidade dos serviços de TI com base em critérios de disponibilidade, segurança e desempenho.

Prevenir e mitigar riscos que possam impactar a execução contratual, o orçamento institucional e a integridade das informações.

Estabelecer ações corretivas e preventivas para os riscos identificados.

Garantir conformidade com as normas legais, regulatórias e contratuais.

3. METODOLOGIA

A identificação e análise dos riscos foram realizadas com base em:

- Análise documental do ETP e dos termos de referência;
- Estimativa de probabilidade e impacto para cada risco identificado;
- Classificação do nível de risco (Baixo, Médio ou Alto);
- Definição de ações de mitigação, prevenção e monitoramento.

4. MATRIZ DE RISCOS

Risco Identificado	Probabilidade	Impacto	Nível de Risco	Ações de Mitigação
1. Atraso na entrega dos serviços de segurança (NGFW, antivírus, suporte técnico) - Lote 1	Média	Alto	Alto	Cronograma detalhado; Monitoramento contínuo da execução; Cláusulas de penalidade e glosas.
2. Atraso na implantação dos serviços de data center em nuvem privada - Lote 2	Média	Alto	Alto	Definir cronograma de implantação; Fiscalização e auditoria técnica para garantir cumprimento dos prazos.
3. Falhas de segurança e vazamento de dados sensíveis - Lotes 1 e 2	Baixa	Muito Alto	Alto	Exigir cláusulas de confidencialidade e conformidade com a LGPD.
4. Desempenho abaixo do esperado da infraestrutura em nuvem privada - Lote 2	Média	Médio	Médio	Auditoria periódica do desempenho; Aplicação de penalidades contratuais.
5. Escalonamento de custos e imprevisibilidade orçamentária - Lotes 1 e 2	Baixa	Alto	Médio	Estabelecer valores fixos mensais e cláusulas de reequilíbrio econômico-financeiro.
6. Não conformidade com LGPD - Lotes 1 e 2	Baixa	Muito Alto	Alto	Exigir conformidade com a LGPD; Monitoramento contínuo das práticas de segurança da informação.
7. Interrupção nos serviços essenciais (impacto na continuidade acadêmica) - Lotes 1 e 2	Baixa	Muito Alto	Alto	Redundância e contingência; Realização de testes periódicos de continuidade operacional.

Essa análise ajuda a identificar quais riscos possuem maior prioridade de tratamento, com base na combinação da sua probabilidade de ocorrência e impacto sobre o projeto. Riscos com maior probabilidade de materializar aliado a variável alto impacto, devem ser tratados com maior urgência e atenção.

5. MONITORAMENTO E REVISÃO

A gestão dos riscos será responsabilidade da equipe de fiscalização contratual da Diretoria de Tecnologia da Informação e Inovação da Universidade Municipal de São Caetano do Sul, em conjunto com os demais membros da equipe técnica. As ações incluem:

- Reuniões periódicas de acompanhamento da execução contratual;
- Aplicação de checklists de conformidade e auditoria técnica;
- Registro de incidentes e providências no sistema ITSM da Universidade;
- Revisão da matriz de risco semestralmente ou quando identificada alteração de cenário.

6. CONCLUSÃO

O presente plano visa garantir que os serviços contratados estejam alinhados com as melhores práticas de governança, segurança e continuidade operacional, preservando os interesses públicos e garantindo a efetividade da contratação. O acompanhamento sistemático dos riscos permitirá uma atuação preventiva e corretiva, reduzindo a possibilidade de prejuízos à administração pública.

7. APROVAÇÃO E ASSINATURA

O Plano de Gerenciamento de Riscos deverá ser assinado pela Equipe de Planejamento da Contratação, nas fases de Planejamento da Contratação e de Seleção de Fornecedores, e pela Equipe de Fiscalização do Contrato, na fase de Gestão do Contrato.

_____

Alessandro Parada

Diretor de Tecnologia da Informação e Inovação