CO-02.06/2026

PROCESSO SEI Nº 7010.2026/0005402-3

MODALIDADE DE CONTRATAÇÃO: CONTRATAÇÃO EMERGENCIAL – Dispensa de Licitação nº 06.004/2026.

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE SOC (SECURITY OPERATIONS CENTER), SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT), IMPLEMENTAÇÃO, SERVIÇO TÉCNICO ESPECIALIZADO, EM CARÁTER EMERGENCIAL.

CONTRATANTE: EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP S/A, com sede na Rua Líbero Badaró nº 425, Centro, no Município de São Paulo, no Estado de São Paulo, CEP 01.009-905, inscrita no CNPJ sob o nº 43.076.702/0001-61, neste ato representada por seu Diretor de Administração e Finanças, Sr. **LUCIANO FELIPE DE PAULA CAPATO**, portador da Cédula de Identidade RG nº 26.277.697-2-SSP/SP e inscrito no CPF/MF sob o nº 025.401.959-54 e por seu Diretor de Relacionamento e Inteligência de Mercado, Sr. **TIAGO MIGUEL DA SILVA LUZ**, portador da cédula de identidade RG nº 4.644.200-8-SSP/SP e inscrito no CPF/MF sob nº 285.192.178-93.

CONTRATADA: CLARO S.A., com sede na Rua Henri Dunant, nº 780, Torre A e Torre B, bairro Santo Amaro, Município de São Paulo, Estado de São Paulo, CEP 04.709-110, inscrita no CNPJ sob nº 40.432.544/0001-47, neste ato representada por **PAULO ROGÉRIO DOS SANTOS**, brasileiro, portador da Cédula de Identidade RG nº 14263890-0-SSP/SP e inscrito no CPF/MF sob o nº 091.756.318-22, e **ANA LUCIA DOMIQUILI**, brasileira, portadora da Cédula de Identidade RG nº 19885247-2 SSP/SP e inscrita no CPF/MF sob nº 131.549.948-74.

As partes acima qualificadas resolveram, de comum acordo, celebrar o presente contrato, mediante as seguintes cláusulas e condições:

CLÁUSULA I – OBJETO

1.1. O presente contrato tem por objeto **prestação de serviços de SOC (Security Operations Center), SIEM (Security Information and Event Management), Implementação, Serviço Técnico Especializado, em caráter EMERGENCIAL,** conforme descrições constantes no Termo de Referência – ANEXO I, da Proposta Comercial da CONTRATADA e demais documentos constantes do processo administrativo em epígrafe**.**

CLÁUSULA II – OBRIGAÇÕES DA CONTRATADA E CONTRATANTE

2.1. São obrigações da CONTRATADA:

a) Cumprir fielmente todas as obrigações estabelecidas no **Termo de Referência – ANEXO I** deste instrumento, garantindo a qualidade dos serviços prestados;

b) Para a assinatura do Instrumento Contratual, a CONTRATADA deverá apresentar todos os documentos relativos à regularidade fiscal, e ainda estar em situação regular junto ao CADIN (Cadastro Informativo Municipal) do **Município de São Paulo (Lei Municipal n.º 14.094/2005 e Decreto Municipal n.º 47.096/2006**), mediante consulta ao site http://www3.prefeitura.sp.gov.br/cadin/.

c) Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de qualificação exigidas no momento da contratação, podendo a CONTRATANTE exigir, a qualquer tempo durante a vigência do contrato, a comprovação das condições que ensejaram sua contratação, devidamente atualizadas e o envio das certidões a seguir elencadas, em formato digital (arquivo PDF) para o e-mail contratosfornecedores@prodam.sp.gov.br e para o gestor do contrato a ser definido oportunamente:

i. Certidão Negativa de Débitos relativa aos Tributos Federais e a Dívida Ativa;
ii. Certidão de Regularidade do FGTS (CRF);
iii. Certidão Negativa de Débitos Tributários e da Dívida Ativa Estadual;
iv. Certidão Negativa de Débitos de Tributos Municipais (Mobiliários);
v. Certidão Negativa de Débitos Trabalhistas (CNDT);
vi. Certidão Negativa de Falência ou Recuperação Judicial.

d) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responderá por danos causados, nos termos do art. 76 da Lei nº 13.303/2016;
e) Dar ciência imediata e por escrito a CONTRATANTE de qualquer anormalidade que verificar na execução do contrato;
f) Prestar a CONTRATANTE, por escrito, os esclarecimentos solicitados e atender prontamente as reclamações sobre a execução do contrato;
g) Responder pelos encargos trabalhistas, previdenciários, fiscais, comerciais e tributários, resultantes da execução deste contrato, nos termos do **artigo 77, da Lei Federal nº 13.303/16**.

2.2. São obrigações da **CONTRATANTE**:

a) Exercer a fiscalização do contrato, designando fiscal (is) pelo acompanhamento da execução contratual; procedendo ao registro das ocorrências e adotando as providências necessárias ao seu fiel cumprimento, tendo por parâmetro os resultados previstos no contrato
b) Fornecer à CONTRATADA todos os dados e informações necessários à execução do contrato;
c) Efetuar o pagamento devido, de acordo com o estabelecido neste contrato.
d) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;
e) Comunicar a CONTRATADA formalmente (por e-mail) todas e quaisquer ocorrências relacionadas com a prestação dos serviços objeto deste Contrato.

CLÁUSULA III – VIGÊNCIA CONTRATUAL

3.1. O contrato terá vigência de **180 (cento e oitenta) dias**, contados a partir da data de sua assinatura, nos termos do artigo 29, inciso XV, da Lei nº 13.303/16.

3.2. Qualquer alteração e/ou acréscimos ou supressões que vierem a ocorrer no decorrer deste contrato será objeto de termo aditivo, previamente justificado e autorizado pela CONTRATANTE.

3.3. O presente contrato será rescindido, mediante prévia comunicação no prazo de 30 (trinta) dias corridos, em razão da conclusão do procedimento licitatório regular destinado à contratação definitiva do objeto e o início da respectiva execução contratual pela empresa vencedora, sem que disso decorra qualquer direito à indenização, ressalvados os pagamentos devidos pelos serviços efetivamente prestados até a data da extinção contratual.

CLÁUSULA IV – PREÇO

4.1. O valor total do presente contrato é de **R$ 953.178,42 (novecentos e cinquenta e três mil, cento e setenta e oito reais e quarenta e dois centavos)**, conforme proposta comercial acostada aos autos (doc. 158469910) e seguirá as regras previstas na **Cláusula VI – Faturamento e Condições de Pagamento**.

4.2. No valor acima já estão incluídos todos os tributos e encargos de qualquer espécie que incidam ou venham a incidir sobre o preço do presente contrato.

CLÁUSULA V – GARANTIA CONTRATUAL (Art. 70, §1º da Lei Federal nº 13.303/16)

5.1. A CONTRATADA deverá prestar garantia contratual no prazo máximo de 15 (quinze) dias a contar da assinatura do contrato, na forma do **artigo 70, § 1º da Lei Federal nº 13.303/16**, no valor de **R$ 47.658,92 (quarenta e sete mil, seiscentos e cinquenta e oito reais e noventa e dois centavos)**, correspondente a 5% (cinco por cento) do valor contratado, observando os procedimentos a seguir elencados.

5.2. A garantia, qualquer que seja a modalidade escolhida, deverá abranger um período mínimo de três meses após o término da vigência contratual, devendo a garantia assegurar a cobertura de todos os eventos ocorridos durante a sua validade, ainda que o sinistro seja comunicado depois de expirada a vigência da contratação ou validade da garantia.

5.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

5.3.1. Prejuízos advindos do inadimplemento total ou parcial do objeto do contrato.
5.3.2. Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo da CONTRATADA durante a execução do contrato.
5.3.3. Multas, moratórias e compensatórias, aplicadas pela CONTRATANTE.
5.3.4. Obrigações trabalhistas e previdenciárias relacionadas ao contrato e não adimplidas pela CONTRATADA.

5.4. A CONTRATADA deverá informar, expressamente, na apresentação da garantia, as formas de verificação de autenticidade e veracidade do referido documento junto às instituições responsáveis por sua emissão.

5.5. No caso de seguro-garantia, a instituição prestadora da garantia contratual deve ser devidamente autorizada pela Superintendência de Seguros Privados – SUSEP e, no caso de fiança bancária, pelo Banco Central do Brasil.

5.6. A insuficiência da garantia não desobriga a CONTRATADA quanto aos prejuízos por ela causados, responsabilizando-se por todas as perdas e danos apurados pela CONTRATANTE que sobejarem aquele valor.

5.7. Para cobrança pela CONTRATANTE de quaisquer valores da CONTRATADA, a qualquer título, a garantia poderá ser executada, a partir do 3º (terceiro) dia, contado da resposta NÃO CONHECIDA E/OU IMPROCEDENTE acerca da notificação judicial ou extrajudicial à CONTRATADA, na hipótese do não cumprimento de suas obrigações contratuais.

5.7.1. Se o valor da garantia for utilizado, total ou parcialmente, cobrança de penalidade aplicada ou pagamento de qualquer obrigação da CONTRATADA, deverá ser efetuada a reposição do valor no prazo de 15 (quinze) dias úteis, contados da data em que for notificada para fazê-lo.

5.8. Caso haja aditamento contratual que implique alteração do valor, a garantia oferecida deverá ser atualizada.

5.9. Não sendo a garantia executada por força de penalidade administrativa e não havendo débitos a saldar com a CONTRATANTE, a garantia prestada será devolvida ao término do contrato.

5.10. Quando prestada em dinheiro, a garantia será devolvida por meio de depósito em conta bancária e corrigida pelos índices da poupança, salvo na hipótese de aplicações de penalidades pecuniárias ou necessidade de ressarcimento de prejuízos causados pela CONTRATADA à CONTRATANTE ou a terceiros, hipóteses em que será restituído o saldo remanescente.

5.10.1. Na hipótese de garantia em dinheiro, a CONTRATADA deverá enviar uma cópia do depósito bancário para o e-mail contratosfornecedores@prodam.sp.gov.br, identificando o contrato e a que título foi realizado o depósito.

CLÁUSULA VI – FATURAMENTO E CONDIÇÕES DE PAGAMENTO

6.1. CONDIÇÕES DE FATURAMENTO

6.1.1. O valor dos itens 1 e 2 Tabela de Composição de Itens será faturado mensalmente em parcelas iguais, a partir da emissão do "Termo de Aceite dos Serviços de SOC e SIEM";

6.1.2 O valor do item 3 da Tabela de Composição de Itens será faturado em parcela única, a partir da emissão do "Termo de Aceite do Serviço de Implementação e Ativação de SOC e SIEM";

6.1.3 O valor do item 4 da Tabela de Composição de Itens, será faturado mensalmente, conforme consumo de horas utilizado e justificado pela CONTRATADA e aprovado pela CONTRATANTE.

6.2. CONDIÇÕES DE PAGAMENTO

6.2.1. A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, através do setor de Expediente, por meio do endereço eletrônico gfl@prodam.sp.gov.br.

6.2.1.1. Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CONTRATANTE disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, aprovando os serviços prestados.

6.2.1.2. O pagamento das parcelas mensais será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pela Gerência de Planejamento e Controle Financeira (GFP), em 90 (noventa) dias corridos a contar da data de emissão do Termo de Aceite de Pagamento.

6.2.1.3. Caso a Nota Fiscal Eletrônica de Serviços contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de Serviços, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.

6.2.1.4. Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% "*pro-rata tempore*"), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

CLÁUSULA VII – MATRIZ DE RISCOS

7.1. Tendo como premissa a obtenção do melhor custo contratual mediante a alocação do risco à parte com maior capacidade para geri-lo e absorvê-lo, as partes identificam os riscos decorrentes da presente relação contratual e, sem prejuízo de outras previsões contratuais, estabelecem os respectivos responsáveis na Matriz de Riscos constante no **ANEXO IV** parte integrante deste contrato.

7.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados, na Matriz de Riscos, como de responsabilidade da CONTRATADA.

CLÁUSULA VIII – CONFORMIDADE

8.1. A CONTRATADA, com relação às atividades, operações, serviços e trabalhos vinculados ao objeto do presente contrato, declara e garante o cumprimento dos dispositivos da **Lei Anticorrupção – Lei 12.846/2013, e dos dispositivos 327, *caput*, § § 1º e 2º e 337-D do Código Penal Brasileiro**

8.2. A CONTRATADA deverá defender, indenizar e manter a CONTRATANTE isenta de responsabilidade em relação a quaisquer reivindicações, danos, perdas, multas, custos e despesas, decorrentes ou relacionadas a qualquer descumprimento pela CONTRATADA das garantias e declarações previstas nesta cláusula e nas Leis Anticorrupção.

8.3. A CONTRATADA reportará, por escrito, para o endereço eletrônico a ser fornecido oportunamente, qualquer solicitação, explícita ou implícita, de qualquer vantagem pessoal feita por empregado da CONTRATANTE para a CONTRATADA ou para qualquer membro da

CONTRATADA, com relação às atividades, operações, serviços e trabalhos vinculados ao objeto do presente contrato.

8.4. Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma, nos termos do **Decreto n.º 56.633/2015.**

8.5. O descumprimento das obrigações previstas nesta Cláusula poderá submeter à CONTRATADA à rescisão unilateral do contrato, a critério da CONTRATANTE, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a **Lei Federal nº 12.846/2013.**

CLÁUSULA IX – DA PROTEÇÃO DE DADOS

9.1. A **CONTRATADA**, obriga-se, sempre que aplicável, a atuar no presente Contrato em conformidade com a legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, não colocando, por seus atos ou por omissão a **PRODAM-SP** em situação de violação das leis de privacidade, em especial, a **Lei nº 13.709/2018 – Lei Geral de Dados Pessoais ("LGPD").**

9.2. Caso exista modificação dos textos legais acima indicados ou de qualquer outro, de forma que exija modificações na estrutura do escopo deste Contrato ou na execução das atividades ligadas a este Contrato, a **CONTRATADA** deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a **PRODAM-SP** poderá resolvê-lo sem qualquer penalidade, apurando-se os serviços prestados e/ou produtos fornecidos até a data da rescisão e consequentemente os valores devidos correspondentes.

9.3. A **CONTRATADA** se compromete a:

i) Zelar pelo uso adequado dos dados aos quais venha a ter acesso, cuidando da sua integridade, confidencialidade e disponibilidade, bem como da infraestrutura de tecnologia da informação;

ii) Seguir as instruções recebidas da **PRODAM-SP** em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, sob pena de arcar com as perdas e danos que eventualmente possa causar à **PRODAM-SP**, aos seus colaboradores, clientes e fornecedores, sem prejuízo das demais sanções aplicáveis;

iii) Responsabilizar-se, quando for o caso, pela anonimização dos dados fornecidos pela **PRODAM-SP;**

iv) A **CONTRATADA** deverá notificar a **PRODAM-SP** em 24 (vinte e quatro) horas de **(i)** qualquer não cumprimento (ainda que suspeito) das obrigações legais relativas à proteção de Dados Pessoais; **(ii)** qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; e **(iii)** qualquer violação de segurança no âmbito das atividades da **CONTRATADA**;

v) A **CONTRATADA** deverá notificar a **PRODAM-SP** sobre quaisquer solicitações dos titulares de Dados Pessoais que venha a receber, como, por exemplo, mas não se limitando, a questões como correção, exclusão, complementação e bloqueio de dados, e sobre as ordens de tribunais, autoridade pública e regulamentadores competentes, e quaisquer outras exposições ou ameaças em relação à conformidade com a proteção de dados identificadas pelo mesmo;

vi) Auxiliar a **PRODAM-SP** com as suas obrigações judiciais ou administrativas aplicáveis, de acordo com a LGPD e outras leis de privacidade aplicáveis, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança.

9.4. A **CONTRATADA** deverá manter registro das operações de tratamento de Dados Pessoais que realizar, bem como implementar medidas técnicas e organizacionais necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado para o tratamento de Dados Pessoais é estruturado de forma a atender os requisitos de segurança, os padrões de boas práticas de governança e os princípios gerais previstos na legislação e nas demais normas regulamentares aplicáveis.

9.5. A **PRODAM-SP** terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da **CONTRATADA** com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição da responsabilidade que a **CONTRATADA** possui perante a LGPD e este Contrato.

9.6. A **CONTRATADA** declara conhecer e que irá seguir todas as políticas de segurança da informação e privacidade da **PRODAM**, bem como realizará treinamentos internos de conscientização a fim de envidar os maiores esforços para evitar o vazamento de dados, seja por meio físico ou digital, acidental ou por meio de invasão de sistemas de software.

9.7. O presente contrato não transfere a propriedade de quaisquer dados da **PRODAM-SP** ou dos clientes desta para a **CONTRATADA**.

9.8. A **PRODAM-SP** não autoriza a **CONTRATADA** a usar, compartilhar ou comercializar quaisquer eventuais elementos de dados, que se originem ou sejam criados a partir do tratamento de Dados Pessoais, estabelecido por este Contrato.

CLÁUSULA X – SANÇÕES ADMINISTRATIVAS

10.1. A CONTRATADA está sujeita às penalidades previstas na **Lei Federal nº 13.303/16**, sem prejuízo da apuração de perdas e danos, em especial:

a) Advertência por escrito;

b) **Multa de até 10% (dez por cento**) sobre o valor total do instrumento contratual ou da parcela correspondente, se o serviço prestado estiver em desacordo com as especificações contidas no **Termo de Referência – ANEXO I** do Edital;

c) **Multa de 1%** (um por cento) sobre o valor total do instrumento contratual, ou parcela equivalente, pelo descumprimento de qualquer outra condição fixada neste contrato e não abrangida nas alíneas anteriores, e na reincidência, o dobro, sem prejuízo da responsabilidade civil e criminal que couber;

d) **Multa de 20% (vinte por cento)** sobre o valor total do instrumento contratual, no caso de rescisão e/ou cancelamento do contrato por culpa ou a requerimento da CONTRATADA, sem motivo justificado ou amparo legal, a critério da CONTRATANTE.
e) **Suspensão** temporária de participação em licitação e **impedimento** de contratar com a PRODAM-SP, pelo prazo de até 02 (dois) anos.
f) Demais sanções encontram-se enumeradas no item 9 do Termo de Referência – ANEXO I.

10.2. Para a cobrança, pela CONTRATANTE, de quaisquer valores da CONTRATADA, a qualquer título, a garantia contratual prevista neste instrumento poderá ser executada na forma da lei.

10.3. Previamente a aplicação de quaisquer penalidades a CONTRATADA será notificada pela CONTRATANTE a apresentar defesa prévia, no prazo de 10 (dez) dias úteis, contados do recebimento da notificação que será enviada ao endereço eletrônico indicado no preâmbulo do contrato ou na proposta comercial. Fica facultado à CONTRATADA o envio da defesa prévia e do recurso administrativo por meio eletrônico.

10.4. A aplicação de penalidade de multa não impede a responsabilidade da CONTRATADA por perdas e danos decorrente de descumprimento total ou parcial do contrato.

10.5. A aplicação de quaisquer multas pecuniárias não implica renúncia, pela PRODAM-SP, do direito ao ressarcimento dos prejuízos apurados e que sobejarem o valor das multas cobradas.

10.6. As decisões da Administração Pública referentes à efetiva aplicação da penalidade ou sua dispensa serão publicadas no Diário Oficial Cidade de São Paulo, nos termos do **Decreto Municipal nº 62.100/22**.

CLÁUSULA XI – RESCISÃO

11.1. A **PRODAM-SP** poderá rescindir o presente contrato, nos termos do **artigo 473, do Código Civil**, nas seguintes hipóteses:

a) Inexecução total do contrato, incluindo a hipótese prevista no **artigo 395, parágrafo único do Código Civil;**
b) Atraso injustificado no início do serviço;
c) Paralisação do serviço, sem justa causa e prévia comunicação à **PRODAM-SP**;
d) Cometimento reiterado de faltas na sua execução que impeçam o prosseguimento do contrato;
e) Transferência, no todo ou em parte, deste contrato, sem prévia e expressa autorização da CONTRATANTE;
f) Decretação de falência;
g) Dissolução da sociedade;
h) Descumprimento do disposto no **inciso XXXIII do artigo 7º, da Constituição Federal**, que proíbe o trabalho noturno, perigoso ou insalubre a menores de 18 anos e qualquer trabalho a menores de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;
i) Prática pela CONTRATADA de atos lesivos à Administração Pública previstos na **Lei nº 8.429/1992 (Lei de Improbidade Administrativa) e Lei nº 12.846/2013 (Lei Anticorrupção);**
j) Prática de atos que prejudiquem ou comprometam a imagem ou reputação da PRODAM, direta ou indiretamente;

11.1.1. A rescisão a que se refere esta cláusula, deverá ser precedida de comunicação escrita e fundamentada da parte interessada e ser enviada à outra parte com antecedência mínima de 10 (dez) dias.

11.2. Desde que haja conveniência para a **PRODAM-SP**, a rescisão amigável é possível, por acordo entre as partes devidamente reduzido a termo no competente processo administrativo.

11.3. Poderá haver também rescisão por determinação judicial nos casos previstos pela legislação.

11.4. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

11.5 Não constituem causas de rescisão contratual o não cumprimento das obrigações aqui assumidas em decorrência dos fatos que independam da vontade das partes, tais como os que configurem caso fortuito e força maior, previstos no **artigo 393, do Código Civil**.

11.6 Os efeitos da rescisão do contrato serão operados a partir da comunicação escrita, ou, na impossibilidade de notificação do interessado, por meio de publicação oficial; ou da decisão judicial, se for o caso.

CLÁUSULA XII – DISPOSIÇÕES GERAIS

12.1. Os termos e disposições deste contrato prevalecerão sobre quaisquer outros entendimentos ou acordos anteriores entre as partes, explícitos ou implícitos, referentes às condições nele estabelecidas.

> **12.1.1** O presente instrumento e suas cláusulas se regulam pela **Lei Federal nº 13.303/16**, pelos preceitos de direito privado, mormente a **Lei n. 10.406/02 (Código Civil)** e disposições contidas na legislação municipal, no que couber.

12.2. A CONTRATADA deverá, sob pena de rejeição, indicar o número deste contrato nas faturas pertinentes, que deverão ser preenchidas com clareza, por meios eletrônicos, à máquina ou em letra de forma.

12.3. A inadimplência do contratado quanto aos encargos trabalhistas, fiscais e comerciais não transfere à empresa pública ou à sociedade de economia mista a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato ou restringir a regularização e o uso das obras e edificações, inclusive perante o Registro de Imóveis.

12.4. A mera tolerância do descumprimento de qualquer obrigação não implicará perdão, renúncia, novação ou alteração do pactuado.

12.5. Na hipótese de ocorrência de fatos imprevisíveis que reflitam nos preços dos serviços, tornando-o inexequível, poderão as partes proceder a revisão dos mesmos, de acordo com o disposto no **artigo 81, § 5º, da Lei Federal nº 13.303/16**.

12.6. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e o CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

12.7. A formalização do presente contrato abrange as disposições contratuais e de todos os seus anexos.

CLÁUSULA XIII – VINCULAÇÃO AO PROCESSO ADMINISTRATIVO

13.1. O cumprimento deste contrato está vinculado aos documentos que instruíram o **Processo SEI nº 7010.2026/0005402-3** e seus anexos e à proposta da CONTRATADA.

CLÁUSULA XIV – FORO

14.1. As partes elegem o Foro Cível da Comarca da Capital de São Paulo, com renúncia de qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas que possam surgir no decorrer da execução deste contrato.

E por estarem assim, justas e contratadas, assinam as partes o presente instrumento em 2 (duas) vias de igual teor, perante 2 (duas) testemunhas abaixo.

São Paulo/SP, 03 de junho de 2026.

gov.br Documento assinado digitalmente
LUCIANO FELIPE DE PAULA CAPATO
Data: 08/06/2026 16:04:14-0300
Verifique em https://validar.iti.gov.br

CONTRATANTE:

LUCIANO FELIPE DE PAULA CAPATO
Diretor de Administração e Finanças

gov.br Documento assinado digitalmente
TIAGO MIGUEL DA SILVA LUZ
Data: 08/06/2026 18:41:45-0300
Verifique em https://validar.iti.gov.br

TIAGO MIGUEL DA SILVA LUZ
Diretor de Relacionamento e Inteligência de Mercado

CONTRATADA:

PAULO ROGÉRIO DOS SANTOS
Representante legal

gov.br Documento assinado digitalmente
PAULO ROGERIO DOS SANTOS
Data: 03/06/2026 16:14:01-0300
Verifique em https://validar.iti.gov.br

ANA LUCIA DOMIQUILI
Representante legal

gov.br Documento assinado digitalmente
ANA LUCIA DOMIQUILI
Data: 03/06/2026 17:49:27-0300
Verifique em https://validar.iti.gov.br

TESTEMUNHAS:

1. gov.br Documento assinado digitalmente
JOSE RICARDO VICENTE
Data: 08/06/2026 09:27:47-0300
Verifique em https://validar.iti.gov.br

2. gov.br Documento assinado digitalmente
LUCIANO FRIZENNI
Data: 08/06/2026 09:38:03-0300
Verifique em https://validar.iti.gov.br

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa para prestação de serviços de SOC (Security Operations Center), SIEM (Security Information and Event Management), Implementação, Serviço Técnico Especializado, de forma EMERGENCIAL, para o período de 180 (cento e oitenta) dias.

1.1 TABELA DE COMPOSIÇÃO DOS ITENS

SOC / SIEM / Serviços Técnicos Especializados			
Item	**Descrição**	**Unidade**	**Quantidade**
1	Serviços de Monitoração, Notificação e Resposta a Incidentes de Segurança da Informação (SOC)	UN	01
2	Serviço de Coleta e Correlação de Eventos de Segurança (SIEM)	UN	01
3	Serviço de Implementação e Ativação de SOC e SIEM	UN	01
4	Serviços Técnicos Especializados de Segurança da Informação	Hora	600

1.2 VIGÊNCIA

O contrato emergencial terá vigência de 180 (cento e oitenta) dias, a contar da **data de assinatura do contrato**, com cláusula resolutiva expressa vinculada à conclusão da licitação ordinária em curso (SEI 7010.2026/0000504-9).

2. DA JUSTIFICATIVA

A presente justificativa tem objetivo de demonstrar a necessidade de dar início a procedimento para contratação emergencial dos serviços de SOC (Security Operations Center), SIEM (Security Information and Event Management), Implementação e Ativação e Serviço Técnico Especializado para o período de até 180 dias.

Embora a solução atual de SOC e serviços de apoio para execução de RDM/OS/Incidentes estejam em operação na Prodam, a Diretoria e a Presidência deliberaram pela abertura de um novo processo licitatório para substituição do fornecedor vigente. A Gerência de Infraestrutura e Tecnologia (GIT) foi incumbida de revisar o Termo de Referência e dar andamento ao processo.

Atendendo ao quanto solicitado, demos início ao processo SEI 7010.2026/0000504-9, atualmente em fase de Pesquisa de Preços de Mercado que está sendo realizada pela Gerência de Compras e Contratações (GFC).

Considerando os riscos à qualidade e segurança dos serviços, bem como os prazos envolvidos para a conclusão da licitação em andamento, e conforme solicitação da Presidência e da Diretoria de Infraestrutura e Tecnologia, a fim de mitigar os riscos envolvidos, esta GIT solicita a contratação de empresa que atenda ao objeto em questão com urgência, tendo em

vista a essencialidade dos serviços e, haja visto, que o atual processo licitatório em andamento não será concluído a tempo de permitir a necessária continuidade dos serviços.

Ressaltamos que esta GIT tem por objetivo consultar o maior número possível de empresa para participar da Pesquisa de Preços de Mercado, de modo que os serviços sejam adquiridos dentro da condição mais vantajosa para a administração pública.

A contratação deste novo serviço está alinhada:

- Às boas práticas de gestão, à modernização tecnológica e à busca contínua por eficiência operacional da PRODAM, garantindo maior sustentabilidade financeira e melhor atendimento às demandas da organização;

- À melhoria do nível de segurança cibernética da infraestrutura fornecida à Prefeitura de São Paulo, indo ao encontro da Orientação Técnica - OT 013 DIRETRIZES BÁSICAS DE SEGURANÇA DA INFORMAÇÃO (volume 03) da Secretaria Municipal de Inovação e Tecnologia da PMSP, (DECRETO Nº 57.653 DE 7 DE ABRIL DE 2017 « Catálogo de Legislação Municipal – acesso em 16/01/2026).

3. SOLUÇÃO

3.1. Serviço de Monitoração, Notificação e Resposta a Incidentes de Segurança;

3.1.1. A CONTRATADA deverá prestar Serviço Gerenciado de Segurança, contemplando a operação de um Centro de Operações de Segurança com a gestão de resposta a incidentes de Segurança da Informação utilizando como base o framework NIST3 SP 800-61;

3.1.1.1. Os seguintes framework's também deverão ser utilizados para apoiar o framework NIST SP 800-61:

3.1.1.1.1. Information Technology Infrastructure Library – ITIL 4, ou seja:

3.1.1.1.1.1. A Prática de Gerenciamento de Segurança da Informação;

3.1.1.1.1.2. Segurança no Fluxo de Valor;

3.1.1.1.1.3. Gestão de Mudanças e Segurança;

3.1.1.1.1.4. Gestão de Incidentes de Segurança;

3.1.1.1.1.5. Governança e Conformidade (GRC);

3.1.1.1.2. The NIST Cybersecurity Framework – CSF

3.1.1.1.3. MITRE ATT&CK

3.1.2. A CONTRATADA deverá comprovar aderência a boas práticas de segurança da informação compatíveis com a ISO/IEC 27001, ou seja, executar o contrato em ambiente que possua, no mínimo:

3.1.2.1. Gestão de riscos de segurança da informação;

3.1.2.2. Políticas formais de segurança;

3.1.2.3. Controles para proteção de ativos de informação;

3.1.2.4. Tratamento de incidentes;

3.1.2.5. Procedimentos de controle de acesso, logs e auditoria;

3.1.2.6. A CONTRATANTE exercerá a fiscalização de modo trimestral para avaliar a aderência dos itens acima. O não atendimento aos requisitos, acarretará penalidade prevista no item 9.1.8 deste Termo de Referência.

3.1.3. O serviço deve contemplar dois ou mais Centros de Operações de Segurança (SOC) em locais distintos, operando em regime 24x7x365 (vinte e quatro horas

por dia, sete dias por semana, todos os dias do ano), com alta disponibilidade, redundância e continuidade operacional, suportado por modelo de operação distribuída;

3.1.4. A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica:
- 3.1.4.1. Solução de proteção de endpoints;
- 3.1.4.2. Solução de prevenção contra vazamento de informações (DLP);
- 3.1.4.3. Solução de proteção de e-mails;
- 3.1.4.4. Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria;
- 3.1.4.5. Efetuar o registro dos visitantes com identificação individual e controle digital de entrada e saída, mantendo o registro armazenado e disponível para consulta por 90 dias;
- 3.1.4.6. Monitoramento por equipe de segurança patrimonial em regime 24x7x365;
- 3.1.4.7. Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 90 (noventa) dias;
- 3.1.4.8. Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações da CONTRATANTE devem assinar termo de responsabilidade e sigilo;

3.1.5. A solução de monitoramento dos alertas e coleta de logs de segurança em regime 24x7 (24 horas por dia, 7 dias da semana) deverá ser fornecido pela CONTRATADA e poderá ser instalado em ambiente VMWare 8.0, da CONTRATANTE.

3.1.6. A CONTRATADA obriga-se a fornecer ponto de conexão VPN para comunicação de dados, destinado exclusivamente à transferência dos logs necessários às atividades de monitoramento do SOC.
- 3.1.6.1. A referida conexão VPN deverá possuir mecanismo de redundância, garantindo alta disponibilidade e continuidade operacional para os dois sites da CONTRATANTE, de forma ininterrupta.
- 3.1.6.2. Compete à CONTRATADA configurar a VPN em sua infraestrutura, responsabilizando-se por assegurar seu perfeito funcionamento.
- 3.1.6.3. A configuração da VPN na infraestrutura da CONTRATANTE será responsabilidade da equipe técnica da PRODAM.

3.1.7. Deve fornecer controle dos eventos de SOC por meio de solução de gestão de operações de segurança da informação.
- 3.1.7.1. A solução deve possuir integração com a ferramenta de SIEM;
- 3.1.7.2. Estar atualizada e possibilitar acesso às principais funcionalidades, como:
  - 3.1.7.2.1. Dashboards;
  - 3.1.7.2.2. Detalhes de eventos;
  - 3.1.7.2.3. Ferramentas de investigação;
  - 3.1.7.2.4. Gerenciamento de tickets e alertas;
  - 3.1.7.2.5. Relatórios;

3.1.7.2.6. Orquestração de trabalho coordenado em etapas manuais e automatizadas;

3.1.7.3. Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática;

3.1.7.4. Permitir o recebimento de Alertas de Segurança com as seguintes características:

3.1.7.4.1. Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;

3.1.7.4.2. Dados de origem e destino, portas de origem e destino, domínios de origem e destino, endereço MAC de origem e destino, além de informações de contexto de negócios de cada dispositivo (de origem ou destino). As informações de contexto deverão incluir endereço IP, nome do dispositivo, tipo, unidade de negócios, site, índice de criticidade e conformidade, além do proprietário, tanto para os dispositivos de origem quanto dispositivos de destino. É necessário também incluir informações de localização do dispositivo, incluindo cidade, país e geolocalização tanto dos dispositivos de origem quanto dos dispositivos de destino dos alertas;

3.1.7.4.3. A CONTRATADA deverá incluir a equipe técnica da CONTRATANTE nos alertas de segurança da informação, a critério da CONTRATANTE;

3.1.7.5. A solução deverá permitir a rastreabilidade das operações realizadas, referente à ação de tickets e em configurações;

3.1.7.6. Manter o histórico de todas as atividades realizadas pelos usuários, tais como criação de registro e atualizações de campos, vinculando o usuário que realizou cada procedimento;

3.1.7.7. Permitir a consulta e exportação das trilhas de auditoria, logs e históricos;

3.1.7.8. Prover mecanismo de proteção contra alteração e remoção indevida dos registros de auditoria;

3.1.7.9. Permitir a definição de controles de segurança, incluindo as seguintes informações: nome do controle, status de implementação, descrição, proprietário, custo operacional anual, categoria do controle (detecção/prevenção), custo fixo, localização e eficácia do controle ao longo do tempo. Desta forma, deverá ser possível avaliar a efetividade de controles implementados em face a Incidentes e Brechas de Segurança;

3.1.7.10. Permitir atrelar os controles de segurança a incidentes efetivos e inefetivos;

3.1.7.11. Possibilitar a criação de políticas de SOC com a definição de proprietário e descrição dos detalh es, além da definição das partes interessadas;

3.1.7.12. A CONTRATADA deverá fornecer à equipe técnica da CONTRATANTE, acesso em nível leitura à solução de gestão do SOC.

3.1.7.13. Permitir a geração de relatórios manuais e automatizados, possuindo funcionalidade de agendamento e envio por e-mail;

3.1.7.14. Possuir alguns relatórios pré-formatados, e possibilitar a exportação nos formatos CSV, PDF, MHTML, Excel e Word, para no mínimo:

3.1.7.14.1. Incidentes abertos por fase
3.1.7.14.2. Incidentes Encerrados por Duração
3.1.7.14.3. Incidentes Abertos Por Duração
3.1.7.14.4. Incidentes Abertos por severidade
3.1.7.14.5. Incidentes reabertos
3.1.7.14.6. Falso positivo por Solução
3.1.7.14.7. Tempo Médio de resolução por tipo de incidente
3.1.7.14.8. Tempo Médio entre o alerta e o primeiro tratamento por tipo de incidente
3.1.7.14.9. Incidentes com SLA expirado por tipo de Incidente
3.1.7.14.10. Incidentes com SLA expirado por responsável

3.1.8. A CONTRATADA deve realizar as ações necessárias para identificação e solução dos incidentes de segurança por meio dos dados e alertas monitorados em Solução de SIEM, que podem comprometer a segurança dos serviços e ativos da CONTRATANTE. A CONTRATADA deve analisar eventos detectados, classificar e categorizar conforme definição da CONTRATANTE, bem como identificar, registrar, escalar, mitigar e, caso necessário, notificar os incidentes de segurança à CONTRATANTE;

3.1.9. A CONTRATADA é responsável pelas atividades do SOC, que para o modelo definido corresponde minimamente às atividades relacionadas abaixo:

3.1.9.1. Definição de linha base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção.

3.1.9.2. Monitoração de alertas de segurança, onde o analista deve decidir se uma análise é necessária. A detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limiares estabelecidos no baseline. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

3.1.9.2.1. Ataque de força bruta com e sem sucesso;
3.1.9.2.2. Falhas de autenticação que indiquem suspeita de roubo de identidade;
3.1.9.2.3. Infecção de equipamentos por vírus;
3.1.9.2.4. Comprometimento de ativos da rede;
3.1.9.2.5. Realização de ações suspeitas por parte de usuários privilegiados;
3.1.9.2.6. Alertas de operação de serviços, como interrupções e falhas;
3.1.9.2.7. Ataques de negação de serviço;
3.1.9.2.8. Ataques comuns em aplicações WEB, como XSS e SQL injection;
3.1.9.2.9. Atividades de botnets;
3.1.9.2.10. Exploração de vulnerabilidades;

3.1.9.3. Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças.

3.1.9.4. Análise de eventos, onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados. O resultado da análise pode ser uma das seguintes categorias:

3.1.9.4.1. Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes;

3.1.9.4.2. Falso positivo: ocorre quando o sistema detecta incorretamente uma ameaça ou não existe risco no evento detectado, sendo eventos alertados como maliciosos, mas não são;

3.1.9.4.3. Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de segurança, como por exemplo, a análise de vulnerabilidades;

3.1.9.4.4. Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;

3.1.9.5. Registro de análise, todo evento detectado que for selecionado para análise deve ser registrado em Sistema de Ticket, incluindo as atividades de investigação. O resultado da análise pode ser a definição de um falso positivo, encerrando o tíquete, ou a confirmação de um incidente de segurança, escalando o tíquete para tratamento. O tíquete deve conter as seguintes informações:

3.1.9.5.1. Identificador do ticket;

3.1.9.5.2. Sensor que detectou o evento;

3.1.9.5.3. Identificador do evento gerado no sensor;

3.1.9.5.4. Limiar de detecção utilizado para enviar o evento para análise;

3.1.9.5.5. Log do evento detectado;

3.1.9.5.6. Origem e categoria do ataque;

3.1.9.5.7. Data e hora;

3.1.9.6. Triagem e Categorização de eventos, os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado;

3.1.9.7. Padronização de procedimentos de resposta à incidentes, os incidentes devem incluir procedimentos padronizados contendo as melhores práticas para seu tratamento e contenção, de modo que viabilize a execução das medidas corretivas necessárias pela CONTRATADA;

3.1.9.8. Elaboração de relatórios. A CONTRATADA deverá disponibilizar relatórios em formato PDF, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir:

3.1.9.8.1. Classificação dos eventos de segurança;

3.1.9.8.2. Total de eventos avaliados;

3.1.9.8.3. Total de eventos escalados;

3.1.9.8.4. TOP aplicações mais impactadas, TOP origens dos eventos de segurança;

3.1.9.8.5. TOP endereços de destino das ameaças;

3.1.9.8.6. TOP URLs e suas categorias;

3.1.9.8.7. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;
3.1.9.8.8. Principais tipos de ataques;
3.1.9.8.9. Descrição dos casos de uso utilizados para avaliar os alertas de segurança;
3.1.9.8.10. Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, dashboards, assinaturas instaladas, etc;

3.1.9.9. A CONTRATADA será responsável pela execução do processo de resposta a incidentes, conforme definição de tabela de atendimento de níveis de serviços (SLA) descrita no item 6 deste Termo de Referência;

3.1.9.10. A CONTRATADA será responsável pela contenção, mitigação e erradicação de ameaças;

3.1.9.11. A CONTRATADA fornecerá apoio técnico à equipe técnica da CONTRATANTE, durante incidentes críticos;

3.1.9.12. A CONTRATADA realizará periodicamente e de forma iterativa a caça proativa de ameaças (Threat Hunting) no ambiente monitorado da CONTRATANTE, com o objetivo de investigar redes, servidores e sistemas para detectar e isolar ameaças que ultrapassaram as defesas de segurança tradicionais;

3.1.9.12.1. Agendando: o processo de Threat Hunting deverá ser executado, no mínimo semanalmente;
3.1.9.12.2. Por gatilho: o processo de Threat Hunting deverá ser executado sempre que um evento externo ou interno sinalizar um risco potencial;

3.1.10. A CONTRATADA deverá ainda, no mínimo, realizar as seguintes atividades, sem se limitar a elas:

3.1.10.1. Análise de Regras e Políticas de Segurança:
3.1.10.1.1. Objetivo: Avaliar e revisar regras e políticas de segurança em vigor na CONTRATANTE.
3.1.10.1.2. Descrição: Conduzir análises estratégicas de políticas e regras de segurança aplicadas a firewalls, WAF, IPS, endpoints e ativos de rede, utilizando enriquecimento automático de dados para correlacionar eventos brutos com o contexto de identidade, geolocalização e criticidade do ativo.
3.1.10.1.3. Realizar análises forenses e de tráfego de rede sobre dados enriquecidos por threat intelligence, visando à identificação proativa de riscos e à redução de falsos positivos.
3.1.10.1.4. Utilizar os dados contextuais para o aprimoramento e a orquestração de playbooks de resposta a incidentes, garantindo ações de mitigação.
3.1.10.1.5. Implementar, no mínimo os seguintes playbooks:

MITRE	Identificador	Caso de Uso	Playbook de Resposta
Credenciais / Acesso	Brute Force	Tentativas excessivas de login em AD, LDAP, VPN	Reset automático de senha, bloqueio temporário de conta, alerta SOC + notificação ao usuário

Credenciais / Acesso	Privilege Abuse	Uso anômalo de contas privilegiadas / login fora de horário	Revogação automática de token/sessão, bloqueio de credencial e alerta imediato
Execução	PowerShell/Bash	Execução suspeita de scripts ou comandos ofuscados	Bloqueio do processo, isolamento do endpoint via EDR, coleta de evidência para forense
Persistência	Scheduled Task	Criação suspeita de tarefas agendadas/startups persistentes	Remoção automática da persistência, isolamento temporário do host
Defesa Evasiva	Masquerading	Execução de binários com nomes falsos (ex.: svch0st.exe)	Quarentena do arquivo, bloqueio de hash em EDR e SIEM
Comando & Controle	DNS/HTTP IOCs	Comunicação com domínios/IPs maliciosos (C&C)	Bloqueio automático em firewall/proxy, isolamento do host
Ransomware e Malware	Data Encrypted for Impact	Criptografia de Arquivos usando algoritmos simétricos	Isolamento rápido de endpoints/servidores, identificação da variante, verificação de backups e interrupção da criptografia.
E-mail / Phishing	Phishing	E-mails suspeitos com link/anexo malicioso	Quarentena automática de mensagens similares, alerta ao usuário e reset de credencial se clicado
Acesso Inicial e Movimentação Lateral	Initial Access, Lateral Movement	Ataques a servidores web ou serviços expostos (ex: VPN, RDP) com vulnerabilidades não corrigidas. Utilização de serviços de conexão remota.	Investigação de conexões VPN suspeitas, uso indevido de ferramentas de administração (RDP, SSH) e abuso de credenciais (RDP).
Coleta de Dados	Data Staging	Compressão/armazenamento incomum de grandes volumes de dados	Alerta SOC, bloqueio temporário da sessão e investigação
Exfiltração	Exfiltration over Web	Transferência anômala de dados para fora (HTTP/FTP/Cloud não usual)	Bloqueio da sessão, alerta SOC e notificação à equipe de privacidade/segurança (LGPD)

3.1.10.2. Elaboração de Pareceres em Segurança da Informação:

3.1.10.2.1. Objetivo: Produzir relatórios detalhados e fundamentados sobre segurança da informação e analisar o nível de maturidade da estratégia de cibersegurança da CONTRATANTE (gestão de segurança e segurança cibernética).

3.1.10.2.2. Descrição: Realizar estudos e análises aprofundadas sobre aspectos de segurança da informação no ambiente de TIC da CONTRATANTE (on-premises e nuvem), gerar pareceres técnicos que ofereçam recomendações estratégicas baseadas em normas e melhores práticas, além de gap analysis para identificar áreas de melhoria.

3.1.10.3. Planos de Melhoria de Infraestrutura de Segurança:

3.1.10.3.1. Objetivo: Apoiar a melhoria contínua da infraestrutura de segurança.

3.1.10.3.2. Descrição: Auxiliar na elaboração de planos de melhoria que otimizem a segurança da infraestrutura existente. Prestar suporte na implementação de novas medidas de segurança.

3.1.10.4. Elaboração de Projetos Técnicos:

3.1.10.4.1. Objetivo: Desenvolver projetos técnicos destinados a mitigar vulnerabilidades na implantação de novos sistemas de informação, novas plataformas, atualizações de software ou vulnerabilidades detectadas pela CONTRATANTE.

3.1.10.4.2. Descrição: Envolver-se na análise e gestão de vulnerabilidades, com foco em ações preventivas e/ou de remediação. Criar documentação técnica detalhada que aborde as vulnerabilidades identificadas, propondo soluções adequadas.

3.1.10.5. Definição e Implementação de Mecanismos de Monitoramento:

3.1.10.5.1. Objetivo: Estabelecer e implementar novos mecanismos de monitoramento e recursos de segurança.

3.1.10.5.2. Descrição: Propor e integrar novos sistemas de monitoramento que se alinhem com as plataformas de segurança da CONTRATANTE. Garantir a vigilância contínua e a pronta resposta a incidentes.

3.1.10.6. Desenvolvimento de Indicadores de Segurança:

3.1.10.6.1. Objetivo: Desenvolver e implantar novos indicadores de desempenho em segurança da informação.

3.1.10.6.2. Descrição: Criar métricas de segurança que permitam a avaliação contínua do ambiente de TI. Implementar indicadores não previstos anteriormente para cobrir novas ameaças.

3.1.10.7. Procedimentos de Auditoria Forense:

3.1.10.7.1. Objetivo: Fornecer orientações sobre auditorias forenses no ambiente de TIC.

3.1.10.7.2. Descrição: Estabelecer procedimentos padronizados para a realização de auditorias forenses.

3.1.10.8. Resposta a Incidentes de Segurança:

3.1.10.8.1. Objetivo: Apoiar na resposta eficaz a incidentes de segurança.

3.1.10.8.2. Descrição: Oferecer suporte especializado na gestão de incidentes de grande vulto. Coordenar ações de contenção, análise e remediação.

3.1.11. Um Sistema de Ticket deverá ser utilizado para registrar e escalar eventos de segurança, de modo a permitir o registro, envio de notificações e alertas entre as equipes da CONTRATANTE e da própria CONTRATADA;

3.1.12. A CONTRATADA é responsável por avaliar os incidentes após o processo de triagem inicial. Caso o incidente seja confirmado, a CONTRATADA executará os seus processos e procedimentos internos para iniciar as medidas de contenção e correção, incluindo configurações nos sensores de segurança ou outros ativos, sejam em dispositivos da CONTRATANTE OU DA CONTRATADA. A CONTRATADA registrará as ações realizadas no tíquete correspondente ao incidente;

3.1.13. Os analistas da CONTRATANTE devem poder contatar os analistas da CONTRATADA, por telefone, Serviços de Troca de Mensagens ou via Sistema de Ticket, para consulta de informações em caso de qualquer dúvida sobre os eventos e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

3.1.14. A CONTRATANTE é responsável por fornecer informações de negócio adequadas, seguindo a regra do privilégio mínimo e necessidade de conhecer, para melhoria da atividade de monitoramento da CONTRATADA;

3.1.15. A CONTRATANTE pode solicitar, a qualquer momento, a customização dos indicadores e informações sobre incidentes e eventos apresentados nos relatórios. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar a customização. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

3.1.16. Por padrão, não será fornecido nenhum tipo de acesso a dados ou sistemas da CONTRATANTE, além dos estritamente necessários para o serviço de monitoramento que serão armazenados na ferramenta de inteligência;

3.1.17. A CONTRATADA deve prover informação específica sobre ameaças, gerada através de um processo (com coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências), que colocam em perigo ativos de informação ou de tecnologia da CONTRATANTE. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco, permitindo melhorar as táticas de detecção de ataques e configuração dos sensores de segurança. O processo deve resultar ainda em conhecimento utilizado para criação de novos indicadores e auxiliar na detecção de ataques futuros, possibilitando a identificação de ameaças específicas ao ambiente da CONTRATADA;

3.1.18. A CONTRATADA deverá apresentar mensalmente relatório contendo as medições dos indicadores de eficiência de SOC, baseado nos frameworks NIST, MITRE ATT&CK e ISO/IEC 27001, para demonstrar sua capacidade de detectar, analisar, responder e mitigar os incidentes de segurança da CONTRATANTE, com objetivo de buscar a melhoria contínua do serviço prestado, identificar gargalos nos processos e diminuir o tempo de exposição a ameaças;

3.1.18.1. O relatório deverá conter os seguintes resultados:

Indicador	Definição	Objetivo	Resultados esperados
MTTD	Tempo médio necessário para que o SOC identifique um incidente de segurança após o início da atividade maliciosa.	Avaliar a capacidade de detecção de ameaças do SOC.	Excelente < 15 minutos Bom 15 – 60 minutos Baixo desempenho > 1 hora
MTTR	Tempo médio necessário para responder e conter um incidente após sua detecção.	Avaliar a capacidade operacional de resposta a incidentes.	Crítico < 30 minutos Alto < 2 horas Médio < 8 horas

MTTI	Tempo médio gasto para investigar e classificar um alerta de segurança.	Avaliar a eficiência analítica dos analistas de SOC.	Entre 5 – 15 minutos
FPR	Percentual de alertas que são classificados como não sendo incidentes reais.	Avaliar a qualidade das regras de detecção e tuning do SIEM.	Excelente < 10% Aceitável 10 – 30% Ruim > 40%
Taxa de Detecção de Incidentes	Percentual de incidentes identificados pelo SOC em relação ao total de incidentes ocorridos.	Avaliar a eficácia da capacidade de detecção do SOC.	
Volume de Alertas por Analista	Quantidade média de alertas tratados por analista em um determinado período.	Avaliar produtividade operacional da equipe.	
Taxa de Escalonamento	Percentual de incidentes que precisam ser escalados para níveis superiores.	- Maturidade do SOC - Qualidade da triagem inicial.	
Cobertura de Monitoramento	Percentual dos ativos da organização que estão efetivamente monitorados pelo SOC.	Avaliar a abrangência da visibilidade de segurança.	
SLA de Atendimento de Incidentes	Percentual de incidentes tratados dentro dos prazos estabelecidos.	Avaliar conformidade com acordos de nível de serviço.	
Taxa de Automação de Resposta	Percentual de incidentes tratados automaticamente por playbooks ou automação.	Avaliar maturidade do SOC e uso de automação	

3.1.19. A CONTRATADA deve fornecer e, quando solicitado pela CONTRATANTE, apresentar:

3.1.19.1. Boletins periódicos, baseados nas informações de dados globais dos centros de pesquisa de ameaças, contendo novas táticas e técnicas de ataque, vulnerabilidades e mecanismos de proteção de interesse da CONTRATANTE;

3.1.19.2. Relatórios mensais especializados para o ambiente da CONTRATANTE, incluindo informações de inteligência, como as novas vulnerabilidades identificadas, ameaças direcionadas identificadas, indicadores de ataque, reputação de endereços IP e domínios, indicadores sobre o cenário de segurança monitorado;

3.1.19.3. Relatório anual sobre a implementação do plano de ação e de resposta à incidentes;

3.1.19.4. Identificação, análise e compartilhamento de informações de ameaças relevantes e emergentes por meio de indicadores de comprometimento;

3.1.19.5. Todos os custos de atendimentos dos incidentes tratados pelo SOC estarão embutidos neste item, ou seja, não há número mínimo ou máximo para atendimentos de incidentes. Não haverá cobrança extra para este tipo de atendimento, considerando desde a detecção do incidente até a sua remediação e solução definitiva.

3.1.19.6. Todo o suporte e comunicação entre as equipes do SOC com a CONTRATANTE será em língua Portuguesa. Caso seja necessário contato com outros terceiros em outra língua, a CONTRATADA

disponibilizará um funcionário com experiencia técnica que fara a tradução durante todo o período necessário para atendimento da ocorrência.

3.1.20. Alocação de Profissionais para os Serviços de Monitoração, Notificação e Resposta a Incidentes de Segurança da Informação (SOC):

3.1.20.1. Os profissionais do Centro de Operações de Segurança (SOC), em conformidade com as qualificações técnicas exigidas, deverão realizar serviço de monitoração, notificação e resposta a incidentes de segurança da informação.

3.1.20.2. Deverá ser disponibilizado pela CONTRATADA, o Centro de Operações de Segurança (SOC), operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), descritos em sua proposta técnica.

3.1.20.3. Os profissionais responsáveis por realizar o serviço de monitoração, notificação e resposta a incidentes de segurança da informação devem possuir, no mínimo:

3.1.20.4. Experiência comprovada de 02 (dois) anos em monitorar, suportar e realizar a identificação e resposta à incidentes de segurança da informação nos mais diversificados ambientes, provendo recomendações com base nas melhores práticas de segurança da informação;

3.1.20.5. Possuir conhecimento em análise e tratamento de incidentes de segurança da informação;

3.1.20.6. De um dos profissionais do SOC, será exigida a seguinte certificação:

3.1.20.6.1. 01 profissional com certificação EC-Council Certified SOC Analyst (CSA);

3.1.20.7. De dois dos profissionais do SOC, será exigida uma das certificações de segurança da informação abaixo:

3.1.20.7.1. 01 profissional com certificação CISSP;

3.1.20.7.2. 01 profissional com certificação *CompTIA Security+;*

3.1.20.7.3. 01 profissional com certificação *CompTIA CySA+;*

3.1.20.7.4. 01 profissional com certificação *CASP+ ou SecurityX;*

3.1.20.7.5. 01 profissional com certificação *CEH — Certified Ethical Hacker;*

3.1.20.8. De dois dos profissionais do SOC, será exigida uma das certificações de Microsoft abaixo:

3.1.20.8.1. Identity and Access Administrator Associate;

3.1.20.8.2. Security Operations Analyst Associate;

3.1.20.9. A comprovação da capacitação técnica se dará mediante a apresentação de certificado de cada item acima.

3.1.20.10. Os certificados apresentados devem estar válidos e terem sido obtidos ou renovados em data não superior a 5 anos contados da data do pregão;

3.1.20.11. A qualquer momento a CONTRATANTE poderá solicitar a revalidação comprobatória das certificações.

3.1.20.12. A qualquer momento a CONTRATANTE poderá solicitar a comprovação de alocação dos profissionais certificados em atividades ligadas ao contrato;

3.1.20.13. Os profissionais designados para realização do serviço devem possuir no mínimo 03 (três) anos de experiência em serviços de Sustentação

de Infraestrutura e Soluções de Segurança ou em gestão e resposta a incidentes de segurança da informação, contados da data do início das atividades;

3.1.20.13.1. Para comprovação deverá ser apresentado atestado de prestação de serviço ou contrato constando data de início e término da prestação;

3.1.20.14. Todos os certificados e atestados exigidos no item 3.1.20, deverão ser apresentados até 02 (dois) dias úteis, antes da assinatura do contrato.

3.2. Serviço de Coleta e Correlação de Eventos de Segurança (SIEM)

3.2.1. Deve ser fornecido o serviço de ferramenta de coleta e correlação de eventos de segurança da informação;

3.2.1.1. A solução proposta deverá utilizar tecnologias como SIEM, SOAR, Inteligência Artificial, para correlacionar dados de múltiplas fontes, identificar padrões de ataque, detectar anomalias em tempo real e aprimorar a resposta.

3.2.1.2. A solução adotada pela CONTRATADA deverá estar coberta por contratos de suporte que atendam aos SLA's exigidos no item 6 deste termo de referência, bem como atualização de versões do fabricante, durante toda a vigência do contrato de prestação deste serviço;

3.2.2. O serviço deve ser fornecido provendo mecanismo de alta disponibilidade;

3.2.3. A solução poderá ser fornecida de forma On-premise, SaaS ou híbrida;

3.2.3.1. Caso a CONTRATADA opte por solução de forma On-premise deverá fornecer toda a infraestrutura necessária (servidor, software, sistema operacional, licenças) para o seu perfeito funcionamento;

3.2.3.2. A utilização de SaaS estará vinculada ao cumprimento da Resolução CD/ANPD Nº 19, de 23 de agosto de 2024, que trata da transferência internacional de dados.

3.2.4. O Serviço deverá ser dimensionado para suportar o armazenamento de eventos de segurança em banco de dados dedicado, disponibilizando acesso aos logs de forma online via interface web por, no mínimo, 90 dias (hot storage) e 180 dias (cold storage).

3.2.5. O serviço fornecido deve permitir a correlação de eventos provenientes de logs;

3.2.6. Associar, dinamicamente, usuários com os seguintes recursos mínimos:

3.2.6.1. Endereço de IP e nome do computador;

3.2.6.2. Endereço MAC;

3.2.6.3. Identificação do usuário logado;

3.2.7. Ser capaz de integrar em uma única console de visualização, todos os dados de logs coletados;

3.2.8. Permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados coletados;

3.2.9. A solução deve possibilitar a criação automática de regras baseadas em IA (Inteligência Artificial) ou Machine Learning a fim de automatizar o processo de busca de ameaças.

3.2.10. Permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;

3.2.11. Possuir regras de correlação especializadas na detecção de incidentes de segurança.

3.2.12. Dentre as regras de correlação, deverá possibilitar a criação de regras que, a partir dos diversos tipos de logs e flows, cubram os seguintes Casos de Uso:
- 3.2.12.1. Exfiltração de dados;
- 3.2.12.2. Identificação de ações que comprometam dados cobertos pelas regulações LGPD (Lei Geral de Proteção a Dados) ou GDPR (General Data Protection Regulation) com possibilidade de adequações;
- 3.2.12.3. Comunicação de dispositivos internos com sites conhecidos por serem controladores de botnet.

3.2.13. Permitir o agendamento automático e manual de relatórios, com a possibilidade do envio por e-mail;

3.2.14. Coletar diariamente informações de fontes relevantes de inteligência de ameaças (ThreatIntelligence) para pesquisar novos tipos de ameaças.

3.2.15. Integrar com o serviço de inteligência de ameaças (ThreatIntelligence) deverá ter a capacidade de implementar técnicas de reputação categorizadas para no mínimo:
- 3.2.15.1. IP's/URL's mal-intencionados;
- 3.2.15.2. Comportamento de ataque, não se limitando a:
  - 3.2.15.2.1. Recon;
  - 3.2.15.2.2. Weaponize;
  - 3.2.15.2.3. Delivery;
  - 3.2.15.2.4. Exploit;
  - 3.2.15.2.5. Privilege Escalation;
  - 3.2.15.2.6. Defense evasion;
  - 3.2.15.2.7. Credencial Access;
  - 3.2.15.2.8. Discovery;
  - 3.2.15.2.9. Exfiltration;
- 3.2.15.3. Comportamento de malware;
- 3.2.15.4. Comportamento de spam;
- 3.2.15.5. URL's de phishing;
- 3.2.15.6. Atividade de botnet;
- 3.2.15.7. Atividade de C&C – Command&Control;

3.2.16. Integrar com o serviço de inteligência de ameaças (ThreatIntelligence) e deverá processar, normalizar, correlacionar, analisar e armazenar eventos de segurança, de forma escalável, possibilitando análise de ambientes com, no mínimo, 55.000 usuários;

3.2.17. Ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação externos, provenientes da base de conhecimento do fabricante da solução de SIEM, da base de conhecimento da própria CONTRATADA e de terceiros, através do serviço de feeds de inteligência e alertas de ameaças direcionadas;

3.2.18. Ser capaz de detectar, em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:
- 3.2.18.1. proxies anônimos;
- 3.2.18.2. endereços de rede TOR;
- 3.2.18.3. botnets e centros de Comando e Controle;
- 3.2.18.4. malware hosts;
- 3.2.18.5. IP's usados para scan de redes;

3.2.19. Possuir integração completa com a solução de GESTÃO DE OPERAÇÕES DE SEGURANÇA DA INFORMAÇÃO, prevista no item 3.1.7;

3.2.20. Abrir chamados na solução de GESTÃO DE OPERAÇÕES DE SEGURANÇA DA INFORMAÇÃO, de forma automática, sempre que detectar um potencial incidente de disponibilidade ou de segurança;
3.2.21. Permitir a criação de perfis de visualização dos eventos derivados dos dados coletados;
3.2.22. Possuir mecanismo de auditoria através da geração de logs das atividades realizadas na console de gerência e investigação;
3.2.23. Permitir a coleta de logs de forma distribuída e permitir a análise centralizada;
3.2.24. Possuir controle de acesso baseado em papéis e perfis de usuários;
3.2.25. Permitir a geração de relatórios em formatos HTML, PDF ou CSV;
3.2.26. Permitir a construção de relatórios customizados pelo usuário;
3.2.27. Possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos, suportando múltiplos métodos de ingestão de dados, incluindo SYSLOG;
3.2.28. Utilizar formatos de logs/eventos nativos de cada fabricante dos dispositivos de segurança, sem utilizar um tipo de formato exclusivo e restrito, definido pelo fabricante da Solução de SIEM;
3.2.29. Permitir a definição e customização de alertas, relatórios e gráficos;
3.2.30. Ser licenciada para atender, no mínimo, 4.000 (quatro mil) Eventos Por Segundo (EPS) ou 40 (quarenta) ativos, para coleta, processamento, armazenamento e correlacionamento dos eventos, de forma sustentada.
    3.2.30.1. Importante destacar que, dentre os ativos que enviam logs, estão relacionados firewalls, WAF, servidores de Active Directory e servidores de gerenciamento de antivírus, que recebem informações de, aproximadamente, 45.000 (quarenta e cinco mil) estações e servidores.
3.2.31. A solução deverá monitorar a quantidade de EPS contratada, com a obrigação de suportar picos que excedam o quantitativo estipulado, por até 8 dias no ciclo mensal de faturamento, processando o volume excedente até que este seja normalizado, sem incorrer a perda de eventos e sem incorrer em qualquer cobrança adicional por excesso ou bloqueio da solução;
    3.2.31.1. Para assegurar a conformidade com os requisitos de suporte a picos, a solução deverá obrigatoriamente implementar uma camada de mensageria baseada em filas (Buffer/Queue), garantindo a persistência dos eventos excedentes e o processamento posterior conforme a disponibilidade de vazão;
    3.2.31.2. O sistema deverá possuir um módulo de telemetria capaz de emitir notificações automáticas via protocolos padrão (REST/SOAP/API) sempre que o volume contratado for excedido ou quando a capacidade de armazenamento temporário atingir níveis críticos, assegurando total transparência sobre o uso da janela de tolerância de 8 dias.
3.2.32. A solução deve suportar a consolidação dos coletores de logs em um concentrador central;
3.2.33. A solução deve possuir relatórios que suportem a gestão das fontes de eventos, como data sources com erro.
3.2.34. A solução deve permitir a customização de novos relatórios baseados em dados de Logs e Flows de rede.
3.2.35. A solução deve segregar a visualização de relatórios apenas para usuários com a devida permissão;

3.2.36. A solução deve possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;
3.2.37. A solução deve possuir a funcionalidade para resolução de endereços IP, como identificação do país e organização das conexões;
3.2.38. A solução deve possuir um mecanismo de pontuação de risco no momento da análise de logs;
3.2.39. A solução deve permitir que, a partir de uma informação existente, se verifique o log que a gerou.
3.2.40. A solução deve permitir a análise avançada de eventos, podendo correlacionar eventos em uma base histórica;
3.2.41. A solução deve ser capaz de coletar e armazenar todos os logs de ativos de rede e dos dispositivos de segurança, mantendo os dados disponíveis para buscas por, no mínimo, 90 dias (hot storage) e 180 dias (cold storage).
3.2.42. A solução deve ser capaz de coletar os logs dos ativos de rede e dos dispositivos de segurança de forma não intrusiva, sem a necessidade de instalação de agentes nos servidores da CONTRATANTE;
3.2.43. A autodetecção da solução deverá ser capaz de possibilitar a busca de eventos, **no mínimo**, com os seguintes recursos:
    3.2.43.1. Busca em tempo real, baseada em “Google-likekeywords” ou “SQL-likestructured queries”;
    3.2.43.2. Possibilidade de converter os resultados procurados em relatórios ou dashboard/widgets;
3.2.44. Realizar a correlação e a geração de alertas em tempo real;
3.2.45. Suportar a criação de interpretadores (parsers) para a integração de logs não suportados nativamente ou API para integração com a solução;
3.2.46. Suportar a criação de interpretadores (parsers) customizados ou conexões de API customizados para no mínimo 20 sistemas proprietários;
3.2.47. Normalizar todos os logs recebidos de ativos de diferentes fornecedores, num formato comum;
3.2.48. Suportar os logs de pelo menos 300 dispositivos diferentes de fabricantes variados;
3.2.49. Possuir capacidade de coletar e correlacionar logs de sistemas operacionais Windows, Linux, Unix e IBM z/OS;
3.2.50. Ser capaz de coletar e correlacionar logs de diversos tipos de dispositivos, tais como: firewalls, antivírus, IPS, proxies, servidores web, servidores DNS, servidores controladores de domínio, load balancers, roteadores, switches, aceleradores WAN e demais dispositivos de rede a critério da CONTRATANTE; que poderão ser inseridos na ativação do serviço ou durante o período contratual.
3.2.51. Ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SNMP, SSH, Microsoft Windows Remote Management, Microsoft Windows EventLogging API, Network flow, arquivos de logs recebido via FTP, arquivos de logs formatados por delimitadores, ODBC/JDBC, VMWare VI-SDK e CISCO;
3.2.52. Não exigir a adição de agentes ou software nos dispositivos monitorados, exceto quando o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de logs citado no item anterior;
3.2.53. Permitir que os logs/eventos sejam enriquecidos/categorizados com informação de criticidade/severidade;

3.2.54. Notificar através de alertas, comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
3.2.55. Gerar alertas baseados no recebimento de logs dos ativos monitorados, pelo menos, das seguintes ameaças:
  3.2.55.1. Host scans, portscans, scans negados, repentino aumento ou redução do tráfego de/para certos endereços IP's;
  3.2.55.2. Anomalias de Logon – excessivas falhas de logon, logon fora do expediente, logon a partir de endereços IP's não usuais;
  3.2.55.3. Bloqueio de contas e passwordscans;
  3.2.55.4. Botnets, worms e outros zero-daymalwares, através do cruzamento dos logs de DNS, DHCP e web proxy;
3.2.56. As regras de correlação da solução deverão permitir a detecção de thresholds ou utilizar testes e operadores lógicos para correlacionar eventos diferentes, permitindo:
  3.2.56.1. Correlação por detecção de anomalia e padrão de comportamento;
  3.2.56.2. Possibilitar a execução automática de scripts, a serem executados em casos "match" com a regra de correlação;
  3.2.56.3. Possibilitar a configuração de política de notificação em cada regra;
  3.2.56.4. O ajuste fino de regras de correlação, permitindo identificar as regras mais acionadas por eventos (que geram mais alertas);
3.2.57. Possuir um painel de controle (Dashboard), onde possa ver o log/evento coletado;
3.2.58. Fornecer painel de controle (Dashboard) que constantemente mostre o status do ambiente de correlação de eventos;
3.2.59. Possuir um dashboard integrado, com os seguintes recursos mínimos:
  3.2.59.1. Visão consolidada das métricas de segurança, para todos os ativos de rede monitorados;
  3.2.59.2. Customização do dashboard, adicionando relatórios e métricas, a critério da CONTRATANTE.
  3.2.59.3. Análise dos eventos de segurança da informação em tempo real;
  3.2.59.4. Análise permitindo detalhá-la a partir de um gráfico geral, descendo aos níveis da análise conforme necessidade;
3.2.60. Ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;
3.2.61. Permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;
3.2.62. Oferecer uma administração centralizada que permita realizar investigações, gestão de incidentes, gestão de alertas e gestão de relatórios.
3.2.63. Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;
3.2.64. Suportar o recebimento de informações de pacotes de rede (Flow) coletados por ferramentas de terceiros, sendo capaz de analisar e correlacionar de forma contínua os dados recebidos;
3.2.65. Ter a habilidade de receber logs/eventos oriundos de um relay de syslogs;
3.2.66. Possuir serviço de monitoração de estado de recebimento e/ou processamento de logs/eventos;
3.2.67. Possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo.
3.2.68. Suportar de forma automática o armazenamento online (dados presentes no storage da solução) e Offline (dados presentes em sistemas de armazenamento off-line, backup, para possível restauração online);

3.2.69. Possuir recurso para tratar dados arquivados e/ou recuperados;
3.2.70. Ser baseada em plataforma WEB, com acesso via browser padrão de mercado, utilizando comunicação criptografada (HTTPS/TLS, versão 1.2 ou superior);
3.2.71. Suportar integração nativa com tecnologia de análise comportamental de entidade e usuário (UEBA), baseado em técnicas de machinelearning ou inteligência artificial, e análises estatísticas para a monitoração de segurança, devendo extrair os dados de usuário e entidades, ações executadas dos eventos coletados para geração de score de risco. A solução deve ser entregue com regras de correlação de análise de comportamento de usuários e entidades prontas para uso, devendo processar e analisar a mesma volumetria solicitada para os outros componentes do SIEM quando aplicável, ou devem considerar o total de 55.000 contas monitoradas (contas de usuários + contas de serviços), monitoração de desvios de comportamento de usuário identificando, no mínimo:
    3.2.71.1. Acesso negado repetido;
    3.2.71.2. Usuário acessando a VPN a partir de uma localidade atípica;
    3.2.71.3. Usuário acessando a VPN a partir de horários atípicos;
    3.2.71.4. Conta utilizada numa quantidade atípica de atividades;
    3.2.71.5. Acesso a endereços considerados suspeitos por bases de Threatfeed/IP Reputation;
    3.2.71.6. Conta de usuário criada e deletada rapidamente;
    3.2.71.7. Detecção de ataque de negação de serviço pela deleção de contas;
    3.2.71.8. Conta anômala em Cloud, criada a partir de uma nova localização;
3.2.72. Permitir identificar a data e hora do último login, de forma a garantir que a credencial não esteja sendo compartilhada;
3.2.73. Permitir o processamento de informações estruturadas de ameaças STIX™ (“StructuredThreatInformationeXpression”);
3.2.74. Possuir um ambiente de construção de regras que ofereça um mecanismo de testes (debug), visando a redução de erros de lógica e sintaxe;
3.2.75. Permitir a customização de perfis de visualização de eventos de acordo com o objetivo da investigação;
3.2.76. Permitir a pesquisa de eventos em Alertas, Incidentes ou Listas.
3.2.77. Permitir automação de fluxos de trabalho (playbooks), incidentes, via SOAR ou IA;
    3.2.77.1. Scripts serão permitidos como ferramenta de auxílio na automação do SOAR ou IA;
3.2.78. Oferecer interface gráfica para criação e edição de playbooks;
3.2.79. Orquestrar respostas a incidentes de segurança de forma automática;
    3.2.79.1. A orquestração e respostas a incidentes automatizada deverá iniciar, no mínimo com 10 regras implementadas, sem limites de novas regras durante a execução do contrato, sendo entre estas:
    3.2.79.2. Resposta a ataques de IP's maliciosos
    3.2.79.3. Bloqueio de usuários privilegiados com movimentação suspeita
    3.2.79.4. Bloqueio de movimentação lateral de malware
    3.2.79.5. Bloqueio de múltiplos hosts infectados pelo mesmo arquivo
    3.2.79.6. Bloqueio de hosts com múltiplos malwares
    3.2.79.7. Bloqueio de contas de serviços sob ataques
3.2.80. A solução deve integrar-se nativamente ou via API aos ativos da CONTATANTE;
    3.2.80.1. A solução deve suportar integração com ferramentas de segurança e TI (firewall, EDR, antivírus, IAM, ITSM, e-mail, entre outras);

3.2.81. A solução deve registrar histórico de ações automatizadas e manuais;
3.2.82. A solução deve possibilitar gestão de incidentes, evidências e indicadores;
3.2.83. A solução deve permitir atuação humana (human-in-the-loop) quando necessário.

3.3. Serviço de Implementação e Ativação de SOC e SIEM

3.3.1. Serviços de implementação da solução de SOC e SIEM contempla planejamento e customização de toda solução executado pela CONTRATADA atendendo os requisitos da CONTRATANTE; e será pago em parcela única e somente no início do projeto após aceite formal da CONTRATANTE, mesmo que haja aumento na quantidade de EPS.
3.3.2. Todas as atividades relacionadas à implementação ocorrerão sob a responsabilidade e expensas da CONTRATADA, sem nenhum ônus adicional para a CONTRATANTE, cabendo a este somente o apoio técnico e a avaliação dos resultados, nos termos previstos neste Edital;
3.3.3. Por implementação e customização entendam-se todos os procedimentos relacionados às parametrizações e testes de quaisquer componentes das soluções ofertadas especificadas no escopo deste Edital, de modo a garantir o pleno funcionamento dos mesmos;
3.3.4. Todos os componentes requeridos para atender às funcionalidades exigidas neste Edital devem estar especificados na proposta;
3.3.5. A CONTRATADA deve criar e manter atualizada a documentação das atividades, dos processos, testes, homologação, entrega e conferência, encontros de trabalho, compromissos e prazos, incluindo planos de trabalho, atas de reuniões, de modo a compor uma documentação final da implantação a ser entregue à CONTRATANTE no final do processo;
3.3.6. A CONTRATADA será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados aos serviços de apoio a customização e implementação da solução, objeto deste Edital. Caso o diagnóstico aponte para problemas não relacionados aos serviços de apoio a customização e implementação da solução, a CONTRATANTE deverá executar os referidos procedimentos, desde que devidamente comprovados pela CONTRATADA, e a critério da CONTRATANTE.
3.3.7. A CONTRATADA deve, às suas expensas, alocar toda a equipe que irá executar os serviços de implementação descritos neste Edital;
3.3.8. Deverão ser alocados, pela CONTRATADA, profissionais qualificados para acompanhar o planejamento e a execução dos serviços de implementação dos componentes da solução;
3.3.9. A equipe alocada pela CONTRATADA deverá realizar as atividades do projeto, no mínimo, nas quantidades de horas descritas abaixo:
3.3.9.1. Profissionais com PERFIL TÉCNICO: 8 (oito) horas diárias, cada um, em horário comercial, durante todo o período de PLANEJAMENTO e EXECUÇÃO da implementação e integração da solução, desde a construção da versão inicial do Plano de Implantação até a emissão do Termo de Aceite;
3.3.9.2. Profissional com PERFIL GERENCIAL: 8 (oito) horas diárias, em horário comercial, durante todo o período de PLANEJAMENTO da implementação e integração da solução, desde a construção da versão inicial do Plano de Implementação, até a emissão do Termo de Aceite;

3.3.10. Dentre os profissionais alocados, a CONTRATADA deverá indicar um Gerente de Projetos, com certificação PMP – Project Management Professional do PMI – Project Management Institute ou possuir MBA – Master of Business Administration em Gerência de Projetos, que será o líder e responsável pela entrega dos serviços e pela implantação e integração da solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital;

3.3.11. Todas as despesas referentes a transporte, alimentação, hospedagem e demais despesas operacionais da equipe alocada pela CONTRATADA ocorrerão às suas expensas;

3.3.12. A CONTRATADA disponibilizará acesso aos recursos computacionais e de apoio técnico às atividades de implementação, desde que absolutamente dentro do escopo das atividades da equipe da CONTRATANTE e a seu critério.

3.3.13. Redefinições durante a implementação serão formalizadas por escrito e justificadas tecnicamente, com atualização do planejamento/cronograma, mantendo-se a premissa de que não haverá alteração de escopo;

3.3.14. A CONTRATADA deve apresentar à CONTRATANTE, em reunião própria, documento que balizará o acompanhamento de todo o projeto de implantação, em formato de Cronograma de Gantt, detalhando todas as fases, atividades, ações, recursos envolvidos (humanos e materiais), prazos, interdependências entre fases, atividades e ações, linha crítica temporal da implementação e quais serão os produtos gerados para cada fase, atividade e ação;

3.3.15. A CONTRATADA deve submeter o Plano de Implementação à homologação por parte da CONTRATANTE, reservando-se este o direito de requerer os ajustes necessários, observadas as melhores práticas amplamente aceitas no mercado e a realidade de seu ambiente;

3.3.16. A CONTRATADA deve englobar, no Plano de Implementação, todos os ajustes que venham a ser solicitados pela CONTRATANTE e apresentar a nova versão;

3.3.17. Os serviços de implementação contemplarão, pelo menos, a realização das seguintes macro-fases:

3.3.17.1. Homologação de funcionalidades da solução em ambiente controlado;

3.3.17.2. Implementação da solução em ambiente de produção;

3.3.17.3. Período de funcionamento experimental;

3.3.18. O Gerente de Projetos da CONTRATADA deve comunicar ao gestor da CONTRATANTE, responsável pelo acompanhamento da implementação dos serviços, a conclusão de cada macro-fase;

3.3.19. O plano de implementação deve considerar os seguintes prazos:

Nº	EVENTO	RESPONSÁVEL		PRAZO MÁXIMO (dias úteis)	A PARTIR DO FIM DO EVENTO
		CONTRATANTE	CONTRATADA		
1	Assinatura do contrato	X	X	--	
2	Entrega da versão inicial do plano de implantação		X	4	1
3	Entrega da versão final do plano de implantação		X	3	2

4	Termo de aceite do plano de implantação	X		1	3
5	Homologação dos Serviços de SOC	X	X	10	3
6	Implementação dos Serviços de SOC		X	13	3
7	Termo de aceite dos Serviços de SOC	X		5	6
8	Homologação dos Serviços de SIEM	X	X	25	3
9	Implementação dos Serviços de SIEM		X	30	3
10	Termo de aceite dos Serviços de SIEM	X		5	9

3.4. Serviços Técnicos Especializados de Segurança da Informação

3.4.1. Este item define um banco de horas de serviços técnicos especializados de segurança da informação, com utilização e pagamento sob demanda, durante a vigência contratual, sem garantia de execução em sua totalidade.

3.4.1.1. O valor estimado de consumo mensal é, em média, de 100 horas;

3.4.1.2. O consumo mensal será baseado nas atividades efetivamente executadas e validadas pela Contratante.

3.4.1.3. Todas as atividades previstas para execução, bem como o tempo estimado, estão previstas no ANEXO I.

3.4.2. Os serviços técnicos deverão ser executados por profissionais qualificados e sempre considerando as melhores práticas do mercado, incluindo normas e regulamentações.

3.4.2.1. Conhecimento pleno de ferramentas de segurança, como SIEM, EDR, DLP, firewalls, antivírus e sistemas de detecção de intrusão (IDS/IPS);

3.4.2.2. Compreensão dos diferentes tipos de ameaças cibernéticas e suas características;

3.4.2.3. Conhecimento de frameworks de segurança, como o NIST Cybersecurity Framework;

3.4.2.4. Conhecimentos em segurança cibernética, redes e sistemas operacionais;

3.4.2.5. Capacidade de análise e investigação de incidentes de segurança;

3.4.3. Atendimento à Atividades de Operação da Segurança da Informação

3.4.3.1. Administração, gerenciamento dos Serviços de Segurança da Informação, por meio de equipe especializada de segurança, abrangendo a totalidade de infraestrutura de segurança e usuários da CONTRATANTE;

3.4.3.1.1. As ferramentas em uso pela CONTRATANTE para a prestação dos serviços poderão ser alteradas durante a vigência do contrato, sempre respeitando os requisitos técnicos mínimos definidos nesta especificação. Neste caso a CONTRATADA participará do processo de implantação da nova ferramenta, devendo providenciar treinamento aos seus profissionais para a continuidade da prestação dos serviços.

3.4.3.2. Todas as atividades que sejam de atendimento à operação de Segurança da Informação, serão originadas por meio da ferramenta de ITSM da CONTRATANTE.

3.4.3.3. Todos os serviços de atendimento de atividades de operação da Segurança da Informação, serão solicitados por meio de ordem de serviço (OS), requisições de mudanças (RDM) e incidentes, abertos

pela ferramenta de ITSM da CONTRATANTE e serão avaliadas e executados de acordo com os níveis de serviços definidos no ANEXO I.

3.4.3.3.1. A CONTRATANTE acompanhará a execução das atividades nos 3 (três) primeiros meses de contrato para ajustes dos serviços aos SLA's desejados.

3.4.3.3.2. Todas as atividades executadas no atendimento às atividades de operação da Segurança da Informação, deverão contribuir para a construção de um Playbook.

3.4.3.3.3. Ocorrerão reuniões semanais entre as equipes da CONTRATANTE e CONTRATADA para alinhamento das atividades, resultados e expectativas.

3.4.3.3.4. Será responsabilidade da Contratada contato com clientes internos e externos para atendimento e validação das demandas.

3.4.4. Prazos

3.4.4.1. Item 1 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento em horário comercial (8 x 5), em dias úteis, sob demanda.

3.4.4.2. Item 2 - Serviços Técnicos Especializados de Segurança da Informação, com atendimento 24 x 7 x 365 (24 horas por dia, sete dias por semana, 365 dias por ano), sob demanda.

3.4.5. Execução das Atividades de Operação da Segurança da Informação

3.4.5.1. No início da execução de cada atividade, a CONTRATADA deverá detalhar e incluir no plano de trabalho as Atividades a serem realizadas, impactos na infraestrutura e arquitetura do ambiente e recomendações para mitigação, caso seja necessário.

3.4.5.1.1. A CONTRATADA deverá iniciar a prestação do serviço no prazo estabelecido na própria ordem de serviço.

3.4.5.1.2. Os serviços serão executados e remunerados de acordo com valor constante da coluna "Ponderação x Tempo de Execução x Convenção SINDPD – formato horas", previamente estabelecido para as atividades, conforme ANEXO I, independentemente do número de profissionais alocados ou do tempo efetivamente gasto na execução dos serviços.

3.4.5.1.3. Os serviços previstos no ANEXO I poderão ser ajustados durante a execução contratual, caso seja verificado que o escopo das atividades é maior ou diferente do que o originalmente previsto nesses documentos. Neste caso, a CONTRATADA poderá solicitar a alteração dos serviços para acréscimo de novas atividades, mediante a apresentação de justificativas.

3.4.5.1.4. A CONTRATANTE, como responsável final pela definição da dimensão dos serviços, analisará as justificativas e emitirá resposta, mesmo nos casos em que as solicitações não forem atendidas. A CONTRATANTE tem o prazo de 3 dias úteis para aprovar o acréscimo de atividades.

3.4.5.1.5. A atualização dos serviços previstos no ANEXO I também poderá ocorrer por iniciativa da CONTRATANTE.

3.4.5.1.6. As alterações podem ocorrer para aumentar ou reduzir o tempo de execução de uma atividade e para incluir ou excluir atividades ao catálogo.

3.4.5.1.7. Caso necessário, a haverá aferição com acompanhamento em tempo integral, por fiscal da CONTRATANTE e técnico conhecedor das tecnologias utilizadas no desenvolvimento da dimensão do escopo, representando a CONTRATADA;

3.4.5.2. Após o término de cada entrega prevista na atividade, a CONTRATADA deverá:

3.4.5.2.1. Apresentar relatório de conclusão dos serviços prestados detalhando todas as atividades realizadas.

3.4.5.2.2. Entregar toda documentação referente aos serviços prestados, contendo todos os documentos produzidos e gerados no contexto da sua execução, anexando à ferramenta ITSM da CONTRATANTE.

3.4.5.3. Os serviços serão prestados pela CONTRATADA remotamente.

3.4.5.3.1. Os serviços podem ser prestados nas dependências da CONTRATANTE, mediante comum acordo entre CONTRATANTE e CONTRATADA, sem ônus adicional para a CONTRATANTE.

3.4.5.3.2. Aqueles serviços que demandarem a presença física de profissionais da CONTRATADA nas dependências da CONTRATANTE deverão ser combinados em comum acordo e agendados previamente.

3.4.6. Local de prestação dos serviços

3.4.6.1. Independentemente dos cenários, dada a sensibilidade das informações tratadas no contexto dos trabalhos do SOC, é vedado o desempenho dessas tarefas em ambientes de trabalho compartilhados, tal como cafés e coworking;

3.4.7. Acesso às plataformas tecnológicas instaladas na CONTRATANTE

3.4.7.1. Controle de Acesso: Todo acesso às plataformas tecnológicas instaladas na CONTRATANTE, necessárias para a prestação dos serviços, será restrito apenas ao pessoal autorizado. Este acesso será realizado exclusivamente por meio de acesso remoto aos recursos da CONTRATANTE, utilizando credenciais de login e autenticação multifator para garantir a segurança.

3.4.7.2. Comunicação Segura: Toda comunicação entre os especialistas da CONTRATADA e as plataformas serão criptografadas. Isso inclui, mas não se limita a comunicações via rede, transferência de arquivos e quaisquer dados trocados entre as partes. A criptografia deve atender aos padrões de segurança mais rigorosos, garantindo a confidencialidade e a integridade das informações.

3.4.8. Requisitos mínimos de experiência profissional:

3.4.8.1. Os profissionais designados para realização do serviço devem possuir no mínimo 03 (três) anos de experiência em serviços de Sustentação de Infraestrutura e Soluções de Segurança ou em gestão e resposta a incidentes de segurança da informação, contados da data do pregão;

3.4.8.2. Para comprovação deverá ser apresentado atestado de prestação de serviço ou contrato constando data de início e término da prestação;

3.4.8.2.1. Os atestados exigidos neste item, deverão ser apresentados até 02 (dois) dias úteis, antes da assinatura do contrato

3.4.9. Visita Técnica:

3.4.9.1. Para a obtenção de informações e condições necessárias à correta elaboração da proposta e execução dos serviços, a licitante poderá realizar visita técnica para tomar conhecimento dos principais softwares, aplicativos, sistemas e ferramentas auxiliares em utilização na Secretaria;

3.4.9.2. O prazo para visita iniciar-se-á no dia útil seguinte ao recebimento deste Termo de Referência, estendendo até o segundo dia útil anterior à data final prevista para o envio da proposta;

3.4.9.3. Para a visita o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da visita;

3.4.9.4. O agendamento deverá ser realizado de segunda a sexta, 8:00 – 12:00 e 13:30 – 17:00, por meio eletrônico e-mail: seginfo@prodam.sp.gov.br;

3.4.9.5. Por ocasião da Visita Técnica acompanhada com o Corpo Técnico, a LICITANTE deverá apresentar a Declaração de Visita Técnica, (ANEXO II) devidamente preenchido e, imediatamente após a visita, a PRODAM deverá providenciar a assinatura da Declaração, por no mínimo, 1 (um) membro do corpo técnico.

3.4.9.6. O licitante que optar pela não realização da visita técnica estará plenamente ciente de que a vistoria foi facultada e que sua não execução implica assumir integralmente os riscos e consequências decorrentes do desconhecimento do ambiente e da infraestrutura envolvida.

4. DAS OBRIGAÇÕES DA CONTRATADA

4.1. Iniciar a prestação dos serviços dentro dos prazos estabelecidos no Edital e seus anexos;

4.1.1. No que diz respeito aos Serviços Técnicos especializados, fica autorizada sua execução imediata e parcial a partir da data da assinatura do contrato, independentemente da homologação dos itens 1, 2 e 3, com base no banco de horas e no atendimento via ITSM.

4.2. A implementação das soluções será realizada pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos da CONTRATANTE;

4.3. A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência, seus anexos e sua proposta comercial, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

4.4. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta comercial, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas para atendimento aos requisitos descritos neste Termo de Referência e em sua proposta;

4.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a

CONTRATANTE autorizada a descontar da garantia, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

4.6. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

4.7. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à CONTRATANTE;

4.8. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique nos ativos da CONTRATANTE envolvidos nos serviços prestados;

4.9. Registrar os tempos de atendimento dos chamados de suporte técnico ou chamados de serviços, indicando os chamados que foram atendidos dentro e fora do ANS estabelecido no Edital e seus anexos;

4.10. Resolver os chamados de serviço e suporte técnico conforme os tempos definidos nas tabelas de tempos de atendimento (SLA) do Edital e seus anexos desde sua detecção até sua mitigação e solução da causa raiz;

4.11. Prestar todo esclarecimento ou informação solicitada pela CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução dos serviços;

4.12. Paralisar, por determinação da CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

4.13. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato;

4.14. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado;

4.15. Submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações deste Termo de Referência;

4.16. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno;

4.17. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

4.18. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

4.19. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da CONTRATANTE;

4.20. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e

tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

4.21. A contratada deverá prestar proteção dos dados a ela compartilhados durante toda a vigência contratual, desde o planejamento dos serviços objeto deste contrato;

4.22. Dentre as rotinas de execução dos trabalhos e etapas a serem executadas a contratada deverá realizar as seguintes atividades:

4.22.1. Executar a integração dos serviços da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega da CONTRATANTE;

4.22.2. Providenciar o planejamento de testes, fornecendo um "Plano de Homologação e Testes" contendo todo o processo de homologação dos serviços e detalhamento dos testes que serão executados para validar a solução implementada;

4.22.3. Executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do serviço, seguindo os procedimentos definidos no "Plano de Homologação e Testes;

4.22.4. Elaborar a "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.

4.23. Durante a implantação da solução, a Contratada deverá realizar, entre outras atividades: instalação de softwares, análise de performance, tunning, resolução de problemas e implementação de segurança.

4.24. Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à implementação da solução.

4.25. A Contratada realizará adequação/configuração do serviço fornecido ao longo da etapa de migração e realização de novas configurações.

4.26. A CONTRATADA deve adotar um modelo de Centro de Operações de Segurança – SOC, prestado em período integral 24x7 (vinte e quatro horas, sete dias por semana) para o tratamento de eventos e incidentes de segurança da informação.

4.27. A medição do serviço será com base em indicadores e nível de serviço mínimo e deverá ser executado pela CONTRATADA, mensalmente, de modo a alcançar as respectivas metas exigidas, conforme INDICADORES DE NIVEL DE SERVIÇOS presente neste Termo de Referência.

4.28. A CONTRATADA deverá fornecer, mensalmente, até o 5º dia útil do mês subsequente à prestação do serviço, em meio eletrônico e em português, relatório detalhado sobre as atividades prestadas pela gestão de incidentes de segurança, geradas a partir do Serviço de Coleta e Correlação de Eventos de Segurança, contendo dados estatísticos pertinentes à gestão de incidentes de segurança, incluindo obrigatoriamente os campos abaixo:

4.28.1. Data/hora do início do evento ou incidente de segurança;

4.28.2. Nome do responsável pelo atendimento;

4.28.3. Descrição do evento ou incidente de segurança;

4.28.4. Severidade;

4.28.5. Número de identificação do chamado;
4.28.6. Descrição da solução realizada;
4.28.7. Tipo de evento ou incidente;
4.28.8. Data/hora de finalização do evento ou incidente de segurança;
4.28.9. Detalhamento do tempo em que o evento ou incidente ficou registrado na solução;
4.28.10. Consolidado dos chamados que não atenderem os prazos estabelecidos no item de INDICADORES DE NÍVEL DE SERVIÇOS, com suas devidas justificativas

4.29. Este relatório é uma obrigação contratual sujeita às sanções previstas no item de CÁLCULO DO NIVEL DE SERVIÇO, o qual deverá ser entregue por meio digital;

4.30. A CONTRATADA deverá fornecer, mensalmente, até o 5º dia útil do mês subsequente à prestação do serviço, em meio eletrônico e em português, relatório detalhado sobre as atividades prestadas para atendimento da operação de segurança da informação, contendo dados estatísticos pertinentes às atividades, incluindo obrigatoriamente os campos abaixo:
4.30.1. Número de identificação do chamado;
4.30.2. Data/Hora início da execução
4.30.3. Nome do responsável pela execução
4.30.4. Descrição de todos os passos executados e suas devidas evidências
4.30.5. Severidade
4.30.6. Data/hora de fim da execução
4.30.7. Planilha com controle de horas utilizadas/disponíveis, conforme total previsto em contrato;

4.31. Este relatório é uma obrigação contratual sujeita às sanções previstas no item de CÁLCULO DO NIVEL DE SERVIÇO, o qual deverá ser entregue no local de execução do contrato.

4.32. Assegurar à CONTRATANTE: Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações;

4.33. Ao término deste contrato, a CONTRATADA deve realizar a transição contratual e efetuar a transferência de todos os dados, documentos e elementos de informação empregados na execução dos serviços, tanto para o CONTRATANTE quanto para a eventual nova contratada.
4.33.1. É de responsabilidade da CONTRATANTE conduzir a transição, devendo, a CONTRATADA, atender às solicitações que digam respeito a transição dos serviços.
4.33.2. As solicitações podem incluir, mas não se resumem à: Participação de reuniões, elaboração de documentos, transferências de senhas e credenciais, templates de configuração das ferramentas, modelos de playbooks, entre outros.
4.33.3. É dever da CONTRATADA desenvolver a documentação minuciosa de cada etapa da transição, a fim de assegurar que as informações, conhecimentos e procedimentos possam ser repassados de maneira precisa e responsável.
4.33.4. A documentação produzida deverá ser aceita formalmente pela CONTRATANTE, para que se caracterize a completa transição, que será

requisito fundamental para o recebimento definitivo do último período de serviço prestado.

5 OBRIGAÇÕES DA CONTRATANTE

5.1 Prover acesso a rede física ou lógica sob demanda;
5.2 Ajustes na rede lógica da Prodam quando necessário;
5.3 Prover informações do ambiente de infraestrutura da Prodam para colaborar na solução de problemas;
5.4 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
5.5 Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
5.6 As funções de gestão e fiscalização do contrato não recairão sobre o mesmo servidor, com as atribuições conforme a seguir especificadas:

5.6.1 Fiscal do Contrato: agirá de forma ativa e preventiva, observando o cumprimento, pela contratada, de todas as regras previstas contratualmente, além de buscar os resultados esperados do pacto com redução efetiva das inconsistências nos procedimentos de sua execução e, ainda, registrar todas as ocorrências relacionadas com a execução do contrato e encaminhar informações ao gestor do contrato.

5.6.2 Gestor do Contrato: irá controlar o processo referente ao contrato, zelando para que constem todos os documentos relativos à contratação, tais como: termo de referência/projeto básico, termo de contrato, ordem de serviço, portarias de nomeação/alteração de fiscal do contrato sempre que ocorrerem termos aditivos, termos de apostilamento, documentos fiscais, liquidações, obrigatoriedade de retenção na fonte dos tributos, entre outros.

5.7 Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;
5.8 Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;
5.9 Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da Contratada, no que couber;
5.10 Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;
5.11 Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;
5.12 Arquivar, entre outros documentos, projetos, as built, especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas.

6 INDICADORES DE NÍVEL DE SERVIÇOS

6.1 A execução dos serviços será gerenciada pela CONTRATADA, que fará o acompanhamento diário da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções de rumo.
6.2 Quaisquer problemas que venham a comprometer o bom andamento das atividades ou o alcance dos níveis de serviço estabelecidos devem ser imediatamente comunicados à CONTRATANTE;

6.3 Tabela com a descrição da severidade de eventos de segurança da informação para atendimento de atividades de SOC e SIEM, não se limitando a isso, podendo a CONTRATANTE alterar, de acordo com a evolução tecnológica e sua necessidade:

Severidade	Descrição
1 – Crítica	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto médio ou alto em qualquer serviço crítico de TI; - Violação significativa de dados sensíveis; - Incidente, em larga escala e/ou longa duração, à disponibilidade e/ou integridade do ambiente; - Vazamento de dados de acordo com a LGPD; - Evidências conclusivas de ataque cibernético.
2 – Alta	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto em grande número de ativos ou ativos de alta criticidade; - Detecção de acesso não autorizado e/ou alterações em sistemas de informação; - Infecção persistente por código malicioso; - Intrusão persistente na rede; - Incidentes de segurança cibernética envolvendo dirigentes; - Ameaça significativa à disponibilidade e/ou integridade do ambiente; - Ameaça significativa à imagem da CONTRATANTE ou seus clientes.
3 – Média	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto em poucos ativos ou um único ativo de média criticidade; - Detecção de varreduras em ativos ou tentativas mal-intencionadas de acesso não autorizado; - Intrusão na rede; - Infecção por código malicioso; - Alterações ou abuso de privilégios; - Ameaça à disponibilidade e/ou integridade do ambiente.
4 – Baixa	Eventos ou incidentes cujo contexto principal é a segurança cibernética, tais como: - Impacto em ativos pontuais ou ativos de baixa criticidade; - Violação das políticas de uso dos recursos tecnológicos; - Ocorrências não confirmadas, potencialmente mal-intencionadas; - Atividades anômalas detectadas na monitoração.

6.4 Os tempos de atendimento máximos toleráveis para atuação dos chamados de SOC e SIEM constam nas tabelas a seguir em horas corridas:

Severidade	Descrição	Prazo Máximo de Detecção (MTTD)	Prazo Máximo de Início de Atendimento (Resposta)	Prazo Máximo de Contenção (MTTR)	Prazo Máximo de Solução
SEVERIDADE BAIXA: A Solução está operativa e a falha não compromete suas	Sistemas operam sem impacto	15 minutos	4 horas	1 dia	2 dias

funcionalidades ou questões não tratadas pela documentação;	ao negócio.				
SEVERIDADE MÉDIA: A Solução está operativa, mas suas funcionalidades são executadas com restrições;	Sistemas operam com degradação de desempenho.	15 minutos	1 hora	12 horas	24 horas
SEVERIDADE ALTA: A Solução está ativa, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;	Sistemas operam com paralisação parcial do ambiente.	15 minutos	30 minutos	6 horas	12 horas
SEVERIDADE CRÍTICA: A Solução está totalmente parada ou inoperante;	Sistemas inoperantes ou paralisação total do ambiente.	15 minutos	10 minutos	1 hora	4 horas
MTTD: Tempo máximo para detecção de uma ocorrência. **Resposta: Tempo máximo para abertura de incidente e início de atuação.** **MTTR: Tempo máximo para adoção de medidas que contenham o problema até que a solução definitiva seja providenciada.**					

6.5 Os tempos de atendimento de Ordens de Serviços, Requisições de Mudanças e Incidentes demandados pelo serviço de ITSM da CONTRATANTE, terão os tempos de atendimento definidos pela própria ferramenta;

6.6 Para fins de fiscalização contratual dos níveis de serviço, os primeiros 90 (noventa) dias do contrato serão considerados período de estabilização e enfrentamento de curva de aprendizado inicial, sendo os níveis de serviços referentes a tal período aferidos, no entanto, no caso da infringência destes, não serão aplicadas as glosas correspondentes.

6.7 O não cumprimento dos prazos e dos critérios de qualidade determinados pelos controles definidos neste Termo de Referência sujeitará a CONTRATADA às glosas e penalidades previstas neste Termo de Referência.

6.8 A frequência de aferição e de avaliação dos níveis de serviço será mensal, devendo a CONTRATADA elaborar relatório gerencial de serviços, contendo a mensuração dos indicadores constantes nas tabelas acima, indicando os demonstrativos e fontes de dados que embasaram tal medição, apresentando-os à CONTRATANTE em condições para que esta possa avaliar a devida aderência dos serviços prestados aos parâmetros de qualidade definidos neste Termo de Referência.

6.9 Devem constar desse relatório gerencial, entre outras informações, também registros de ocorrências relevantes (positivas ou negativas) do período em questão, recomendações técnicas, administrativas e gerenciais para os próximos períodos e quaisquer outras informações relevantes para que a CONTRATANTE tenha subsídios para realizar a devida gestão contratual. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes no primeiro mês de execução do contrato.

6.10 A entrega dos relatórios mensais será condição necessária à atestação dos serviços pela CONTRATANTE.

6.11 Caso algum nível de serviço ou parâmetro de qualidade for infringido, por razões fora da gerência da CONTRATADA, tais ocorrências não constarão do quadro de medições ou de registros negativos de qualidade de execução. No entanto, a CONTRATADA se obriga a descrever o ocorrido, contendo as devidas justificativas motivadoras do porquê não conseguiu contornar o ocorrido sem impacto nos níveis de serviço. Após, a CONTRATANTE avaliará, a cada ocorrência, a aplicabilidade desta cláusula.

6.12 As indisponibilidades programadas por mudanças autorizadas não serão computadas nos Indicadores de desempenho.

6.13 No caso dos indicadores de prazo de atendimento, não serão computados os tempos em que a solicitação aguarda retorno de informações do solicitante ou de equipe externa à gerência da CONTRATADA, ou quando não existirem todos os pré-requisitos disponíveis de imediato.

7 FISCALIZAÇÃO DOS SERVIÇOS

7.1 O acompanhamento dos serviços será executado de acordo com o Regulamento Interno da CONTRATANTE, bem como toda a legislação relacionada.

7.2 O faturamento e o ciclo de fiscalização contratual serão em base mensal.

7.3 A fiscalização requisitante procederá à análise da qualidade dos serviços com base nos parâmetros definidos no item 7 e subitens. Após, emitirá termo de recebimento definitivo, indicando, caso aplicável, se há indicação de descontos ou penalidades contratuais, e assinará aquele termo com o Gestor do Contrato.

7.4 Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.

7.5 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

7.6 Após a apuração do valor devido no período em questão, a fiscalização requisitante informará a CONTRATADA o exato valor para o qual deverá ser emitida a nota fiscal de serviços.

7.7 Se existirem situações para as quais a CONTRATADA não concordar com o valor indicado pela CONTRATANTE como sendo o que deve ser faturado para o período em questão, aquela pode formalizar pedido de revisão, o qual será avaliado pela CONTRATANTE oportunamente e, caso acatado, a diferença será paga no período de faturamento subsequente à conclusão desta análise.

8 CONFIDENCIALIDADE

8.1 A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da Contratante para divulgação;

8.2 Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas de software/hardware contratado ou adquirido sem o conhecimento e formal autorização da Contratante. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

9 PENALIDADES

9.1 Pela inexecução total ou parcial do objeto do Contrato, a CONTRATANTE poderá, garantida a prévia defesa, aplicar a CONTRATADA as seguintes sanções:

9.1.1 Advertência;

9.1.2 Multa de 1% (um por cento) por dia de atraso em qualquer uma das fases previstas no item 3.3 deste Termo de Referência - Serviço de Implementação e Ativação de SOC e SIEM, aplicável sobre o valor do faturamento do item em atraso;

9.1.2.1 Após o 30º (trigésimo) dia de atraso e, a critério da CONTRATANTE, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

9.1.3 Multa aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, pelo não atendimento recorrente dos níveis de serviços relacionados às atividades descritas no item 6 - INDICADORES DE NÍVEIS DE SERVIÇOS e subitem 6.5 (atendimento de Ordens de Serviços, Requisições de Mudanças e Incidentes demandados pelo serviço de ITSM), conforme segue:

9.1.3.1 Será considerado ocorrência faltosa, o atraso no atendimento às atividades demandadas pelo serviço ITSM da CONTRATANTE, superior a 10% (dez por cento) Do total mensal executado pela CONTRATADA;

9.1.3.1.1 Multa de 1% (um por cento) sobre o valor apurado para pagamento no mês;

9.1.3.2 Será considerado ocorrência faltosa, o atraso no atendimento às atividades demandadas pelo serviço ITSM da CONTRATANTE, superior a 20% (vinte por cento) Do total mensal executado pela CONTRATADA;

9.1.3.2.1 Multa de 2% (dois por cento) sobre o valor apurado para pagamento no mês;

9.1.3.3 Será considerado ocorrência faltosa, o atraso no atendimento às atividades demandadas pelo serviço ITSM da CONTRATANTE, superior a 30% (trinta por cento) Do total mensal executado pela CONTRATADA;

9.1.3.3.1 Multa de 5% (cinco por cento) sobre o valor apurado para pagamento no mês;

9.1.3.4 Será considerado ocorrência faltosa, o atraso no atendimento às atividades demandadas pelo serviço ITSM da CONTRATANTE, superior a 40% (quarenta por cento) Do total mensal executado pela CONTRATADA;

9.1.3.4.1 Multa de 10% (dez por cento) sobre o valor apurado para pagamento no mês;

9.1.3.5 Será considerado ocorrência faltosa, o atraso no atendimento às atividades demandadas pelo serviço ITSM da CONTRATANTE, superior a 50% (cinquenta por cento) Do total mensal executado pela CONTRATADA;

9.1.3.5.1 Multa de 20% (vinte por cento) sobre o valor apurado para pagamento no mês e rescisão do contrato;

9.1.3.6 A CONTRATADA será notificada e terá direito à justificativa pelos atrasos apontados, justificativa que será analisada pela CONTRATANTE;

9.1.4 O descumprimento dos prazos de nível de serviço de atendimento previstos no item 6 - INDICADORES DE NÍVEIS DE SERVIÇOS, subitens 5.4, implicará na aplicação de glosas conforme tabela a seguir:

Resultado esperado e níveis de qualidade exigidos	Unidade de Cálculo	Fórmula de Cálculo da Glosa	Limite da Glosa
Urgente / Crítica	1 hora	NHA * 0,1 * VMS	50% do VMS
Alta	1 hora	NHA * 0,05 * VMS	50% do VMS
Normal	1 hora	NHA * 0,02 * VMS	50% do VMS
Baixa	1 hora	NHA * 0,005 * VMS	50% do VMS

Onde:

NHA = Número de Horas de Atraso após o término do prazo máximo esperado para solução.

VMS = Valor Mensal do Serviço (SOC / SIEM)

9.1.5 Multa compensatória correspondente a 5% (cinco por cento), aplicável sobre o preço global do Contrato, caso não seja garantido absoluto sigilo sobre todos os processos, rotinas, objetos, informações, documentos e quaisquer outros dados fornecidos pela CONTRATANTE, além das cominações previstas na legislação, podendo a CONTRATANTE rescindir o Contrato;

9.1.6 Multa de 10% (dez por cento), aplicável sobre o preço global contratado, nas demais violações ou descumprimentos de cláusula(s) ou condição(ões) estipulada(s) no Contrato;

9.1.7 Multa de 10% (dez por cento), aplicável sobre o preço global contratado, em caso de inexecução total do Contrato;

9.1.8 Multa aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, pelo não atendimento de qualquer subitem do item 3.1.2:

9.1.8.1 Multa de 10% (dez por cento) sobre o valor apurado para pagamento no mês;

9.1.9 Suspensão temporária de participar em licitação e impedimento de contratar com a CONTRATANTE pelo prazo de até 2 (dois) anos.

9.1.10 Em caso de penalidades não previstas nos itens 9.1.1 a 9.1.9, será aplicada multa de 0,1% (zero vírgula um por cento) sobre o valor do contrato para cada termo de descumprimento ou cumprimento parcial.

10 QUALIFICAÇÃO TÉCNICA

10.1 A licitante deverá apresentar Atestado(s) de Capacidade Técnica, emitido(s) em papel timbrado por pessoa jurídica de direito público ou privado, que comprove(m) experiência prévia na prestação de serviço de fornecimento de serviços de mesma natureza do presente edital, ou seja, SOC, SIEM e Serviços Especializados de Segurança da Informação.

10.2 Para eventuais esclarecimentos, caso seja necessário durante a licitação, o(s) atestado(s) deverá(ão):

- **Estar devidamente datado(s) e assinado(s)**;
- Conter **identificação clara do atestante** (nome, cargo e empresa/instituição, telefone, e-mail etc.);
- Ser (em) emitido(s) por pessoa jurídica contratante dos serviços prestados.

10.2.1 Será aceita a apresentação de um único atestado ou a somatória de mais de um, desde que, em conjunto, comprovem a execução de serviços pertinentes, compatíveis com o objeto da contratação;

10.2.2 Será aceita a apresentação de atestado(s) emitido(s) em língua estrangeira, desde que acompanhado(s) da devida tradução para língua portuguesa;

10.2.3 Não será aceita a apresentação de atestado(s) emitido(s) por empresas componentes do mesmo grupo econômico da licitante;

10.2.4 Para fins de comprovação de pertinência e compatibilidade, será(ão) considerado(s) válido(s) o(s) atestado(s) que comprove(m) a execução de, no mínimo, os seguintes valores:

10.2.4.1 **50%** (cinquenta por cento) do valor inicial de EPS ou equipamentos, previsto no item 3.2.30 deste Termo de Referência, correspondendo **a 2.000 (dois mil) EPS ou 20 ativos (equipamentos)**;

10.3 A licitante deverá apresentar, juntamente com sua proposta comercial: catálogos, folder, manuais e demais documentos técnicos que comprovem a aderência das soluções às especificações técnicas indicadas no termo de referência.

10.3.1 Para fins de verificação de adequação da solução ofertada as especificações técnicas detalhadas apresentadas neste Termo de Referência deverão ser comprovadas em uma Matriz ponto-a-ponto contendo, de forma organizada, o item do Termo de Referência, O NOME DO ARQUIVO DA DOCUMENTAÇÃO ORIGINAL DO FABRICANTE e a indicação do número da página que comprove o atendimento ao item.

10.3.2 Para comprovações que não constem de catálogos, folder, manuais e demais documentos técnicos, serão aceitas cartas dos fabricantes, destinadas a PRODAM, declarando que cumprem a especificação dos produtos que compõem a solução, com referência explícita a este processo licitatório;

10.4 Para fins de julgamento das propostas a equipe de apoio técnico realizará a conferência técnica dos documentos exigidos, a saber:

10.4.1 Os atestados de capacidade técnica apresentados pelos licitantes em compatibilidade com os serviços realizados, com o objeto licitado, conforme especificado no Termo de Referência;

10.4.2 A verificação será conduzida por equipe de apoio técnico designada, com base nos critérios objetivos descritos no Termo de Referência.

11 ACEITE

11.1 O Termo de Aceite dos Serviços de SOC, SIEM e Atividades de Operação, será emitido mensalmente pela CONTRATANTE, no prazo de até 5 (cinco) dias úteis após a entrega do relatório mensal de atividades, emitido pela CONTRATADA, referente aos serviços prestados pelos itens “Serviços de Monitoração, Notificação e Resposta a Incidentes de Segurança da Informação (SOC)”, “Serviço de Coleta e Correlação de Eventos de Segurança (SIEM)” e “Serviços Técnicos Especializados de Segurança da Informação”, itens1, 2 e 4 da Tabela de Composição de Itens.

11.2 O Termo de Aceite do Serviço de Implementação e Ativação de SOC e SIEM, será emitido pela CONTRATANTE, no prazo de até 5 (cinco) dias úteis após a entrega da formalização, por parte da CONTRATADA, do relatório de implementação contendo a comprovação do pleno funcionamento dos serviços previstos no item 3 da Tabela de Composição de Itens 1.

11.2.1 Entende-se por implementação e ativação a disponibilização de todas as funcionalidades exigidas neste Termo de Referência, inclusive e não se limitando a isso, com a entrega de evidências de registros de construção de automatização de regras de resposta a incidentes.

12 CONSÓRCIO, SUBCONTRATAÇÃO E CESSÃO DE MÃO DE OBRA

12.1 Não haverá cessão de mão de obra.

12.2 Informamos que a Contratação de empresa para prestação de serviços de SOC (Security Operations Center), SIEM (Security Information and Event Management) e Serviço Técnico Especializado, exige uniformidade técnica, responsabilidade única e garantia de continuidade operacional.

12.3 A participação de consórcios ou a subcontratação, com diferentes empresas se responsabilizando por partes distintas da solução, pode acarretar riscos de incompatibilidade entre os componentes, dificuldade na responsabilização técnica por falhas ou problemas operacionais e fragmentação no suporte, dificultando a resolução de incidentes e comprometendo o SLA (Acordo de Nível de Serviço), de modo que, diante de tais riscos técnicos e operacionais é vedada a participação de consórcios no certame e não será permitida a subcontratação do objeto contratual.

ANEXO II

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

A PRODAM – EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO, inscrita no CNPJ nº 43.076.702/0001-61, com sede na Rua Líbero Badaró nº 425 – Centro - São Paulo/SP, doravante denominado CONTRATANTE, e, de outro lado, a **CLARO S.A**., com sede na Rua Henri Dunant, nº 780, Torre A e Torre B, bairro Santo Amaro, Município de São Paulo, Estado de São Paulo, CEP 04.709-110, inscrita no CNPJ sob nº 40.432.544/0001-47, doravante denominada CONTRATADA;

Considerando que, em razão do Contrato nº 02.06/2026 doravante denominado Contrato Principal, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;
Considerando a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;
Considerando o disposto na Política de Segurança da Informação da CONTRATANTE;
Resolvem celebrar o presente Termo de Compromisso de Manutenção de Sigilo, doravante, vinculado ao Contrato Principal, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do Contrato Principal celebrado entre as partes.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtidas por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiro.

Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Parágrafo Primeiro – Serão consideradas como informações sigilosas, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O termo informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao Contrato Principal, doravante denominados Informações, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do Contrato Principal celebrado entre as partes.

Parágrafo Segundo – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do Contrato Principal, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do Contrato Principal.

Parágrafo Terceiro – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do Contrato Principal.

Parágrafo Quarto – As obrigações constantes deste TERMO não serão aplicadas às informações que:

I – Sejam comprovadamente de domínio público no momento da revelação;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

Parágrafo Primeiro – As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Segundo – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Terceiro – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do Contrato Principal

sobre a existência deste TERMO bem como da natureza sigilosa das informações.

Parágrafo Quarto – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quinto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Sexto - A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do Contrato Principal.

Parágrafo Sétimo - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

Parágrafo Único - O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do Contrato Principal.

Cláusula Sexta – DAS PENALIDADES

Parágrafo Único - A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do Contrato Principal firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, previstas nas Leis Federais nº 13.303/2016 e nº 10.520/2002;

Cláusula Sétima – DISPOSIÇÕES GERAIS

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tais como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA referentes à contratação em comento;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao Contrato Principal.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante termo aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais

disponibilizadas, sendo necessário a formalização de termo aditivo ao Contrato Principal;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Parágrafo Quarto – Estabelecidas as condições no presente Termo de Compromisso de Manutenção de Sigilo, a CONTRATADA concorda com os termos da declaração acima, dando-se por satisfeita com as informações obtidas e plenamente capacitada a prestar o serviço contratado.

CO-02.06/2026

ANEXO III

TERMO DE RESPONSABILIDADE DE TERCEIROS E ADESÃO AO CÓDIGO DE CONDUTA E INTEGRIDADE – PRODAM-SP S/A

Nome da empresa: **CLARO S.A**.

CNPJ nº: 40.432.544/0001-47

Vigência contratual: 180 (cento e oitenta) dias, a contar da data de assinatura

Objeto contratual: PRESTAÇÃO DE SERVIÇOS DE SOC (SECURITY OPERATIONS CENTER), SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT), IMPLEMENTAÇÃO, SERVIÇO TÉCNICO ESPECIALIZADO, EM CARÁTER EMERGENCIAL

Declaramos, para os devidos fins, que estamos cientes e concordamos com as normas, políticas e práticas estabelecidas no **CÓDIGO DE CONDUTA E INTEGRIDADE DA PRODAM-SP (https://portal.prodam.sp.gov.br/documents/d/guest/codigo_conduta_integridade_pdf),**res-ponsabilizando-nos pelo seu integral cumprimento, inclusive por parte dos nossos empregados e prepostos, nos termos do artigo 932, III, do Código Civil, comprometendo-nos com a ética, dignidade, decoro, zelo, eficácia e os princípios morais que norteiam as atividades desempenhadas no exercício profissional e fora dele, em razão das obrigações contratuais assumidas, com foco na preservação da honra e da tradição dos interesses e serviços públicos.

ANEXO IV

MATRIZ DE RISCO

Risco	Definição	Alocação (público, privado ou compartilhado)	Impacto (alto, médio, baixo)	Probabilidade (frequente, provável, ocasional, remota ou improvável)	Mitigação (medidas, procedimentos ou mecanismos para minimizar)
Mercado externo	Modificações no fluxo logístico e aduaneiro, e/ou desabastecimento internacional	compartilhado	alto	remota	Modificação dos prazos de entrega e adequação dos modelos de equipamentos, se necessário, adequação do contrato.
Mudanças tributárias	Mudanças na legislação tributária que aumente ou diminua custo, exceto mudança na legislação do IR	Compartilhado	Médio	Remota	Recomposição do equilíbrio econômico financeiro
Modificação da solução	Necessidade de atendimento de itens não previstos na solução	compartilhado	alto	ocasional	Adequação ao contrato
Inovações tecnológicas	Atendimento por parte da CONTRATADA de inovações tecnológicas	compartilhado	baixo	remota	Adequação ao contrato
Variação cambial desproporcional a média apurada em períodos anteriores	Produtos ou componentes não nacionais cotados com base no dólar	Compartilhado	Médio	Ocasional	Reequilíbrio econômico-financeiro mediante a demonstração do impacto dessa circunstância na equação econômico-financeira do contrato

SEI)

061954985

Fundação Theatro Municipal de São Paulo

Diretor Geral: Abraão Mafra
Av. São João, 281 - Centro -
11 33225-8201
E-MAIL: fundacaotmsp@prefeitura.sp.gov.br

DIVISÃO TÉCNICA DE SUPRIMENTOS

Extrato de Aditamento (NP) | Documento: 158816805

PRINCIPAL

Número do Contrato

182

Contratado(a)

LNX TRAVEL VIAGENS E TURISMO LTDA

Tipo de Pessoa

Jurídica

CPF /CNPJ/ RNE

20.213.607/0001-67

Data da Assinatura

02/06/2026

Prazo do Contrato

12

Tipo do Prazo

Mês

Síntese (Texto do Despacho)

Processo nº 8510.2023/0000263-0 - Termo de Aditamento nº 182/FTMSP/2026. Contratante: Fundação Theatro Municipal de São Paulo. Data de Assinatura: 02/06/2026. Contratada: LNX TRAVEL VIAGENS ETURISMO LTDA. CNPJ: 20.213.607/0001-67. Vigência: 01/07/2026 a 01/07/2027. Objeto: Prorrogação contratual - Prestação de serviços de agenciamento de passagens aéreas nacionais, mediante disponibilização de sistema de gestão de viagens corporativas sem alteação do valor anteriormente apostilado.Modalidade de Licitação: Pregão Eletrônico. Fundamento Legal: Lei 14.133/2021. Dotação Orçamentária: 85.10.13.122.4001.2.100.3.3.90.33.00.00. Valor Total: R$ 11.250,00 (onze mil duzentos e cinquenta reais). Número da Nota de Empenho: 422/2026. Valor da Nota de Empenho: R$ 8.437,50 (oito mil quatrocentos e trinta e sete reais e cinquenta centavos). Desembolso no exercício estimado: R$ 8.437,50 (oito mil quatrocentos e trinta e sete reais e cinquenta centavos).

Data de Publicação

09/06/2026

Íntegra do Contrato (Número do Documento SEI)

158806956

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo

Diretor Presidente: Francisco de Padovan Forbes
Rua Líbero Badaró, 425 -
11 3396-9000
E-MAIL: prodam@prodam.sp.gov.br

GERÊNCIA JURÍDICO-CONSULTIVA E GOVERNANÇA CORPORATIVA

Extrato de Contrato/Nota de empenho (NP) | Documento: 158889220

PRINCIPAL

Número do Contrato

CO-02.06/2026

Contratado(a)

CLARO S.A.

Tipo de Pessoa

Jurídica

CPF /CNPJ/ RNE

40.432.544/0001-47

Data da Assinatura

08/06/2026

Prazo do Contrato

180

Tipo do Prazo

Dia

Síntese (Texto do Despacho)

EXTRATO DE TERMO DE CONTRATO. CONTRATO Nº CO-02.06/2026. PROCESSO SEI Nº 7010.2026/0005402-3. DISPENSA DE LICITAÇÃO Nº 06.004/2026. CONTRATANTE: EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO - PRODAM-SP S/A. CONTRATADA: CLARO S.A. (CNPJ: 40.432.544/0001-47). OBJETO: PRESTAÇÃO DE SERVIÇOS DE SOC (SECURITY OPERATIONS CENTER), SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT), IMPLEMENTAÇÃO, SERVIÇO TÉCNICO ESPECIALIZADO, EM CARÁTER EMERGENCIAL. VIGÊNCIA: 180 (CENTO E OITENTA) DIAS, CONTADOS A PARTIR DA DATA DE SUA ASSINATURA. VALOR: O VALOR TOTAL DO PRESENTE CONTRATO É DE R$ 953.178,42 (NOVECENTOS E CINQUENTA E TRÊS MIL, CENTO E SETENTA E OITO REAIS E QUARENTA E DOIS CENTAVOS).

Data de Publicação

09/06/2026

Íntegra do Contrato (Número do Documento SEI)

158889012

Companhia de Engenharia de Tráfego

Presidente: Milton Roberto Persoli
Rua Barão de Itapetininga, 18 - 14º andar - Centro -
11 3396-8301
E-MAIL: presidencia@cetsp.com.br

DEPARTAMENTO DE AQUISIÇÃO DE BENS E SERVIÇOS ESPECIALIZADOS

Outras (NP) | Documento: 158834376

PRINCIPAL

Especificação de Outras

FORMALIZAÇÃO ADITAMENTO Nº 002/2026 REFERENTE AO CONTRATO Nº 066/2023

Síntese (Texto do Despacho)

EXPEDIENTE Nº 920/2022 DESPACHO À vista das informações constantes no expediente, especialmente com base na justificativa da área gestora às fls. 1.131 e 1.165, no Parecer SAJ nº 002/26 às fls. 1.169/1.170 e complementos às fls. 1.176 e 1.180 e com fundamento no disposto no artigo 72 da Lei Federal nº 13.303/16, combinado com o artigo 197 "caput" do Regulamento Interno de Licitações, Contratos e Convênios da CET - RILCC, AUTORIZO o Aditamento ao Contrato nº 066/23, referente à prestação de serviços com fornecimento de plataforma de comunicação SIP, incluindo a gravação das comunicações e plataforma de gerenciamento para ser utilizado pela CET - SP, a ser assinado com a empresa MUNDO TELECOMUNICAÇÕES E INFORMÁTICA LTDA., CNPJ sob o nº 07.403.266/0001-24, para inclusão da cláusula resolutiva:I - A CET poderá rescindir o contrato antecipadamente sem ônus para ela, respeitando-se o cumprimento do aviso prévio que deverá ter seu início comunicado pela CET à CONTRATADA, com 30 (trinta) dias de antecedência, quando da ativação dos equipamentos PABX através da assinatura de um novo contrato, de objeto idêntico ao presente, não cabendo qualquer tipo de indenização à CONTRATADA. II - Publique-se. FORMALIZAÇÃO ADITAMENTO Nº 002/2026 REFERENTE AO CONTRATO Nº 066/2023, celebrado entre a CET e a empresa MUNDO TELECOMUNICAÇÕES E INFORMÁTICA LTDA. - CNPJ Nº 07.403.266/0001-24, referente à prestação de serviços para o sistema de comunicação telefônica da CET - SP, com fornecimento de plataforma e materiais, para acrescentar que A CET poderá rescindir o contrato antecipadamente sem ônus para ela, respeitando-se o cumprimento do aviso prévio que deverá ter seu início comunicado pela CET à CONTRATADA,