



CO-17.12/2025

PROCESSO SEI Nº 7010.2025/0011399-0.

MODALIDADE DE CONTRATAÇÃO: DISPENSA DE LICITAÇÃO Nº 12.018/2025, COM FULCRO NO ARTIGO 29, INCISO XV, DA LEI Nº 13.303/16.

CONTRATO DE FORNECIMENTO DE SERVIÇO PARA SOLUÇÕES DE SEGURANÇA COMPOSTA DE FIREWALL PARA PROVER SEGURANÇA E PROTEÇÃO DE REDES.

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 pelo Diretor de Infraestrutura e Tecnologia, Sr. **THIAGO HENRIQUE SCARABELLO BIROCCHI**, portador da cédula de identidade RG nº 28.970.201-SSP/SP e inscrito no CPF/MF sob nº 270.727.688-07, e pelo 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.

CONTRATADA: TELETEX COMPUTADORES E SISTEMAS LTDA, com sede na Avenida Doutor Cardoso de Melo nº 1308, sala 71, bairro Vila Olímpia, no Município de São Paulo, no Estado de São Paulo, CEP 04.548-004, inscrita no CNPJ sob o nº 79.345.583/0010-33, neste ato representada por sua Procuradora, Sra. **ROBERTA KALINE IORI SANDRI**, portadora da Cédula de Identidade RG nº 8.233.197-2-SESP/PR e inscrita no CPF/MF sob o nº 042.379.249-04.

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 o **FORNECIMENTO DE SERVIÇO PARA SOLUÇÕES DE SEGURANÇA COMPOSTA DE FIREWALL PARA PROVER SEGURANÇA E PROTEÇÃO DE REDES**, 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;

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

Rua Líbero Badaró, 425 – Centro – CEP: 01009-905 – São Paulo – SP





CO-17.12/2025

- 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.

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

Rua Líbero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP





CO-17.12/2025

- 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 **23 de dezembro de 2025**, conforme dispõe o artigo 29, inciso XV, da Lei Federal nº 13.303/2016.

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. Durante o período de vigência, estarão inclusas todas as atualizações necessárias, incluindo as de versões de firmware, atualizações de assinaturas de IPS, Gateway Antivírus/Antispyware, suporte e manutenção.

3.4. Fica assegurado à PRODAM-SP o direito de rescindir o contrato, caso seja realizada nova contratação visando substituí-lo. A rescisão deverá ser precedida de comunicação à CONTRATADA, com antecedência mínima de 30 (trinta) dias.

CLÁUSULA IV – PREÇO

4.1. O valor total do presente contrato é de **R\$ 446.227,56 (quatrocentos e quarenta e seis mil, duzentos e vinte e sete reais e cinquenta e seis centavos)** 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.

4.3. Resta vedado o reajuste do valor contratual por prazo inferior a 12 (doze) meses contados após um ano da data-limite para apresentação da proposta comercial ou do último reajuste, conforme disposto na **Lei Federal nº 10.192 de 14/10/2001**, ou, se novas normas federais sobre a matéria autorizarem o reajustamento antes deste prazo.

4.4. Após o período inicial de 12 (doze) meses de vigência, caso haja prorrogação, o contratado poderá ter seus preços reajustados, aplicando-se a variação do Índice de Preços ao Consumidor IPC/FIPE a contar da data da apresentação da proposta.

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\$ 22.311,38 (vinte e dois mil, trezentos e onze reais e trinta e oito centavos)**, correspondente a 5% (cinco por cento) do valor contratado, observando os procedimentos a seguir elencados.

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

Rua Líbero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP





CO-17.12/2025

- 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.



CO-17.12/2025

- 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 1,2,3 e 4 da tabela de composição de itens do Termo de Referência serão faturados mensalmente, a partir da emissão do "TERMO DE ACEITE", previsto no Item Aceite. O encaminhamento da Nota Fiscal de Serviço deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente ao mês da efetiva prestação dos serviços e autorização do Gestor do Contrato).

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 40 (quarenta) 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

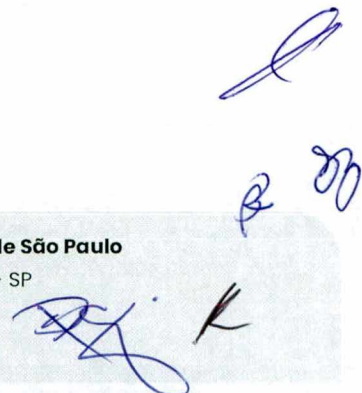
8.1. A CONTRATADA, com relação às atividades, operações, serviços e trabalhos vinculados ao objeto do presente contrato, declara e garante o cumprimento dos dispositivos da **Lei Anticorrupção – Lei 12.846/2013, e dos dispositivos 327, caput, § § 1º e 2º e 337-D do Código Penal Brasileiro**

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 enviaar 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.



CO-17.12/2025

- 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.

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

10.6. 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.

10.7. 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;

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

Rua Líbero Badaró, 425 – Centro – CEP: 01009-905 – São Paulo – SP





CO-17.12/2025

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 nº 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 inexecutável, poderão as partes proceder a revisão dos mesmos, de acordo com o disposto no **artigo 81, § 5º, da Lei Federal nº 13.303/16**.

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

Rua Libero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP





CO-17.12/2025

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 7010.2025/0011399-0** 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, 22 de dezembro de 2025.

CONTRATANTE:


THIAGO HENRIQUE SCARABELLO BIROCCHI
Diretor de Infraestrutura e Tecnologia

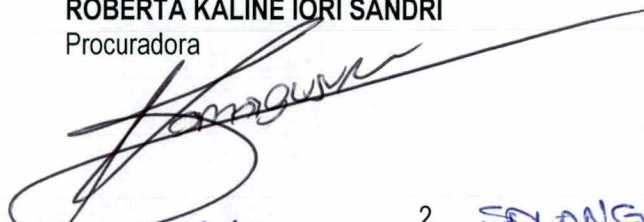

LUCIANO FELIPE DE PAULA CAPATO
Diretor de Administração e Finanças

CONTRATADA:


ROBERTA KALINE IORI SANDRI
Procuradora

TESTEMUNHAS:

1.


RG 18.106.424
CPF 116.302.858-46

2.


SOLANGE R. FARRA
RG 12.621.621
CPF 045.482.338-06

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

Rua Líbero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP



ANEXO I

TERMO DE REFERÊNCIA

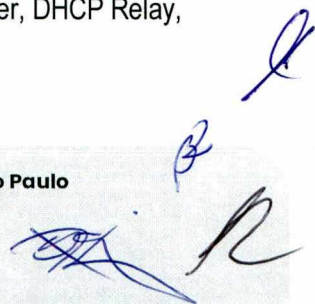
1. OBJETO:

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM TECNOLOGIA DA INFORMAÇÃO PARA FORNECIMENTO DE SERVIÇO PARA SOLUÇÕES DE SEGURANÇA COMPOSTA DE FIREWALL PARA PROVER SEGURANÇA E PROTEÇÃO DE REDES PELO PRAZO DE 180 (cento e oitenta) dias, CONTEMPLANDO OS SEGUINTE SERVIÇOS:

- 1.1. Contratação de solução de segurança com alta disponibilidade de Firewall de nova geração (Next Generation Firewall - NGFW) appliance (hardware dedicado), incluindo sistema de segurança do tipo IDS (Intrusion Detection System), IPS (Intrusion Prevention System), Gateway Anti-Malware bem como suporte, Gerência centralizada, e assistência técnica especializada;
- 1.2. Fornecimento de suporte, manutenção especializada e garantia.

2. ESPECIFICAÇÃO TÉCNICA FIREWALL:

- 2.1 Firewall de nova geração (Next Generation Firewall -NGFW) appliance (hardware), baseado na tecnologia Stateful Packet Inspection com capacidade de Deep Packet Inspection para filtragem de tráfego IP;
- 2.2 Os Firewalls deverão operar em alta disponibilidade;
- 2.3 Deve permitir a configuração dos seguintes modos de operação: transparente mode, Nat mode e routing mode;
- 2.4 Deve permitir o funcionamento em modo transparente tipo bridge e ser configurado em alta disponibilidade neste modo;
- 2.5 Possuir no mínimo 14 (catorze) interfaces de redes com velocidade de 1 Gbps RJ45;
- 2.6 Possuir no mínimo 02 (duas) interfaces de 10 Gbps, SFP+ contendo todos os respectivos transceivers/GBICs no padrão 10 Gb Short Range;
- 2.7 Permitir a criação de, no mínimo, 1024 (mil e vinte e quatro) VLANs, padrão IEEE 802.1Q, definindo interfaces virtuais por identificadores de VLAN (VLAN ID tag). As interfaces virtuais devem permitir as mesmas funcionalidades das interfaces físicas, incluindo designação de zona de segurança, DHCP Server, DHCP Relay, NAT, VPN e regras de controle de acesso;



- 2.8 Possuir suporte a agregação de links 802.3ad (LACP);
- 2.9 Deve permitir a configuração de, no mínimo, 6 (seis) firewalls virtuais, possibilitando o gerenciamento de interfaces, VLAN, zonas, regras, rotas e VPN, de forma individualizada para cada firewall;
- 2.10 Deve possuir capacidade de processamento de, no mínimo, 30 (trinta) Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall ativa, considerando-se para fins de métrica, ambientes de produção (Mundo real);
- 2.11 Deve possuir capacidade de processamento de, no mínimo, 26 (vinte e seis) Gbps (throughput) para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente, considerando-se para fins de métrica, ambientes de produção (Mundo real);
- 2.12 Deve possuir capacidade de processamento de, no mínimo, 15 (quinze) Gbps (throughput) para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações, IPS e Anti-Malware ativas simultaneamente, considerando-se para fins de métrica, ambientes de produção (Mundo real);
- 2.13 Deve possuir performance de VPN IPsec, por appliance, de no mínimo 8 Gbps (throughput) bidirecional, com criptografia 3DES (168 bits) ou AES e pelo menos um túnel de VPN IPsec estabelecido;
- 2.14 Permitir a implementação de no mínimo 10.000 (dez mil) policies;
- 2.15 Possuir capacidade para um mínimo de 12.000.000. (doze Milhões) conexões TCP/IP concorrentes e simultâneas, para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente, considerando-se para fins de métrica, ambientes de produção (Mundo real);
- 2.16 Possuir capacidade para um mínimo de 200.000. (duzentos Mil) novas conexões TCP/IP por segundo, para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente, considerando-se para fins de métricas, ambientes de produção (Mundo real);

Licenças

- 2.17 Deverão ser fornecidas licenças de IPS/IDS, antivírus e antispyware, incluindo licenças para up-dates, com atualização automática para o período contratado, e permitir a possibilidade de renovação das mesmas após seu período de vencimento;

- 2.18 Deverão ser fornecidas licenças de Gateway Anti-Malware, incluindo licenças para updates, com atualização automática e gratuita para o período contratado e permitindo a utilização por um número indefinido de usuários ou endereços IP.
- 2.19 Toda e qualquer licença necessária para completa operação da solução e de suas funcionalidades deverão estar incluso no fornecimento;
- 2.20 Possuir suporte a número ilimitado de endereços IP nas redes internas;
- 2.21 Implementar recurso de NAT (*network address translation*) do tipo um-para-um (*one-to-one*), um-para-muitos (*one-to-many*), muitos-para-um (*many-to-one*) e muitos-para-muitos (*many-to-many*) e tradução simultânea de endereço IP e porta TCP de conexão (NAPT);
- 2.22 Possuir suporte a NAT simétrico;
- 2.23 Suportar NAT em todas as interfaces;
- 2.24 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 2.25 Deverá possuir a função de TOLERANCIA A FALHAS (Alta Disponibilidade), nos modos Ativo/Passivo ou Ativo/Ativo, com todas as licenças de software habilitadas para tal, de forma a garantir que, se um dos firewalls parar de funcionar, o outro deverá assumir automaticamente, suportando todo o tráfego;
- 2.26 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrado no próprio appliance de Firewall;
- 2.27 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;
- 2.28 Deve permitir criar ou importar regras no padrão OpenSource (SNORT), essas regras, devem poder ser habilitadas para simples monitoramento ou para bloqueio de tráfego, não deve haver limite da quantidade de regras a serem criadas ou importadas e não deve haver limite de funcionalidade nas regras criadas ou a serem importadas;
- 2.29 Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 2.30 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
- 2.31 Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão;

IPS

- 2.32 Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura;
- 2.33 Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
 - 2.31.1 Deve permitir o bloqueio de vulnerabilidades.
 - 2.31.2 Deve permitir o bloqueio de exploits conhecidos.
 - 2.31.3 Deve incluir proteção contra-ataques de negação de serviços.
 - 2.31.4 Deverá possuir os seguintes mecanismos de inspeção de IPS:
 - 2.33.4.1. Análise de padrões de estado de conexões;
 - 2.33.4.2. Análise de decodificação de protocolo;
 - 2.33.4.3. Análise para detecção de anomalias de protocolo;
 - 2.33.4.4. IP Defragmentation;
 - 2.33.4.5. Remontagem de pacotes de TCP;
 - 2.33.4.6. Bloqueio de pacotes malformados
 - 2.33.5. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
 - 2.33.6. Detectar e bloquear a origem de portscans;
 - 2.33.7. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
 - 2.33.8. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
 - 2.33.9. Possuir assinaturas para bloqueio de ataques de buffer overflow;
 - 2.33.10. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto, incluído assinaturas customizadas criadas através de um baseline do host, ou seja, deve ser possível construir um padrão de acordo com características do host e caso haja mudança nestas características a solução detectar e/ou aplicar alguma ação de ameaça;
 - 2.33.11. Deverá permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 2.34 Identificar e bloquear comunicação com botnets;
- 2.35 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
 - 2.35.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.36 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação;
- 2.37 Os eventos devem identificar o país de onde partiu a ameaça;

- 2.38 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 2.39 Deve fornecer proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos;
- 2.40 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança.

ANÁLISE DE MALWARES

- 2.41 Devido aos Malwares serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
- 2.42 O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado da solução;
- 2.43 Deve permitir de forma automática a criação e manutenção de um histórico ou fluxo de trabalho forense no qual seja possível identificar:
 - 2.43.1. Inserção de malware no ambiente de rede, movimento lateral, mesmo quando esta não seja detectada inicialmente como malware.
- 2.44 Deve permitir selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 2.45 Deve suportar a monitoração, detecção e prevenção em tempo real de arquivos trafegados nos seguintes protocolos HTTPS, FTP, HTTP, SMTP, IMAP, POP3 como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
- 2.46 Deve permitir especificar o tipo de arquivo, inclusive os comprimidos que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, vlans e outros objetos associados ao controle de acesso do ambiente protegido.
- 2.47 Permitir que seja definido o tamanho máximo dos arquivos a serem inspecionados.

- 2.48 Deve utilizar mecanismo de proteção baseado em reputação global em tempo real, permitindo assim que sejam adotadas ações automáticas de alerta e bloqueio de arquivos suspeitos ou malwares já encontrados anteriormente.
- 2.49 O dispositivo não deve depender ou utilizar de forma exclusiva mecanismos de análise em ambiente virtualizado para que seja feita a detecção e o bloqueio de ameaças malwares em tempo real.
- 2.50 A utilização de recursos de execução virtualizada, não deve depender da configuração manual de imagens ou escolha de versões específicas de sistemas operacionais;
- 2.51 Deve possuir mecanismo blacklist para implementar controles customizados de forma automatizada, incluindo IP, URL'S, entradas de DNS e domínios. IP;
- 2.52 Deve possuir mecanismo whitelist para implementar controles customizados de forma automatizada, incluindo IP, URL'S, entradas de DNS e domínios IP;
- 2.53 Deve possuir capacidade para detecção de Malwares em comunicações de entrada e saída, incluindo a detecção de mecanismos de Comando e Control.
- 2.54 Deve identificar ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de obfuscação e indicadores de comprometimento automáticos.
- 2.55 Deve possuir tecnologia proprietária de execução para verificação de Malwares avançados inclusive mecanismos tipo sandbox.
- 2.56 Deve implementar a identificação e capacidade de controle de acesso em tempo real nos seguintes tipos de arquivo: MSEX, 9XHIVE, DMG, DMP, ISO, NTHIVE, PCAP, PGD, SYLKc, SYMANTEC, VMDK, DWG, IMG_PICT, MAYA, PSD, WMF, SCRENC, UUENCODED, PDF, EPS, AUTORUN, BINARY_DATA, BINHEX, EICAR, ELF, ISHIELD_MSI, MACHO, RPM, TORRENT, AMR, FFMPEG, FLAC, FLIC, FLV, IVR, MIDI, MKV, MOV, MPEG, OGG, PLS, R1M, REC, RIFF, RIFX, RMF, S3M, SAMI, SMIL, SWF, WAV, WEBM, 7Z, ARJ, BZ, CPIO_CRC, CPIO_NEWC, CPIO_ODC, JAR, LHA, MSCAB, MSSZDD, OLD_TAR, POSIX_TAR, RAR, SIS, SIT, ZIP, ZIP_ENC, ACCDB, HLP, MAIL, MDB, MDI, MNY, MSCHM, MSOLE2, MSWORD, MAC5, MWL, NEW_OFFICE, ONE, PST, RTF, TNEF, WAB, WP, WRI, XLW, XPS. Adicionalmente, deve implementar em tempo real a inspeção, detecção e bloqueio autônomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos: 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO_ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEX, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC;

- 2.57 Deve implementar na solução, atualização à base de dados da Rede de Inteligência de forma automática.
- 2.58 Para recursos de análise virtualizada existente, deve ser mantido um histórico dos resultados de avaliações prévias de um arquivo e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite.
- 2.59 Dispor de múltiplos motores e mecanismos de detecção e prevenção para verificação de Malwares e códigos maliciosos incluindo:
- 2.59.1 Machine learning
 - 2.59.2 Reputação global
 - 2.59.3 Detecção customizada local por blacklist e regras customizadas de detecção de tráfego de rede.
- 2.60 Deve possuir capacidade de emular (sandbox) ataques com funcionalidade de APT (Advanced Persistent Threat) e Zero Day em diferentes sistemas operacionais, de forma automática e quando aplicável, tais como:
- 2.60.1 Windows 7, 8, 8.1, 10 e Server 2008 R2, 2012, 2012 R2, 2016;
 - 2.60.2 Linux Red Hat Enterprise Linux ou CentOS 6.x 7.x.
- 2.61 O dispositivo deve ser capaz de enviar arquivos suspeitos de forma automática para análise "In Cloud" ou para dispositivo local, onde o arquivo será executado e simulado em ambiente controlado (Sandbox);
- 2.62 Possibilitar a pré-definição de políticas para determinar quais tipos de arquivos deverão ser enviados para análise;
- 2.63 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para detecção das ameaças não conhecidas;
- 2.64 Deve suportar a monitoração de arquivos trafegados na internet (HTTP, FTP, HTTP, SMTP);
- 2.65 O processo de análise de comunicações, Malwares e sua prevenção deve ocorrer em tempo real, não sendo aceitas tecnologias que dependam de verificações que induzam latência suficiente para postergar a entrega de arquivos ao seu destino original
- 2.66 Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
- 2.67 Suportar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;
- 2.68 Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class);



CO-17.12/2025

- 2.69 Permitir o envio de arquivos para análise no ambiente controlado de forma automática
- 2.70 Permitir a criação de túneis VPN (Virtual Private Network) Site to Site IPSec. Deverão ser incluídas gratuitamente no mínimo 100 licenças para VPN Site to Site;
- 2.71 Suportar protocolo NTP para sincronismo de relógio do equipamento;
- 2.72 Suportar o protocolo SNMP, para checagem de status e TRAP para envio e notificação de alarmes;
- 2.73 Deve possuir suporte completo a protocolos de roteamento (rotas estáticas e dinâmicas IPv4 (BGP e OSPFv2) e IPv6 (BGP e OSPFv3), com possibilidade de programação de rotas para as interfaces;
- 2.74 Permitir a definição de rotas de tráfego baseadas em regras definidas por port de serviço (TCP/UDP) e endereço IP de origem ou destino (PBR – policy based routing);
- 2.75 Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para determinado horário ou período (dia da semana e hora);
- 2.76 Deve possuir fonte de alimentação operando nas tensões 110/220 V, com seleção automática de voltagem e frequência de 50/60 Hz;
- 2.77 Deve possuir fonte redundante;
- 2.78 Possuir estatística de utilização de CPU e memória do firewall;
- 2.79 Possuir no mínimo um disco SSD de 240GB;
- 2.80 O NGFW deve possuir no máximo 3 RU;
- 2.81 Possibilitar a criação de entradas ARP estáticas para fixação de endereço IP com um número MAC específico;
- 2.82 Deverá permitir backup remoto de configuração;
- 2.83 Possuir função de DHCP Server, Relay e Client interno;
- 2.84 Capacidade de enviar e armazenar logs em um servidor remoto via protocolo syslog;
- 2.85 Deverá possuir função de debug on-line, com pesquisa por endereço IP (origem/destino) identificando no mínimo, informações do cabeçalho, porta e protocolo do pacote capturado;

- 2.86 Deverá ser fornecida a versão mais recente para todos os softwares internos dos equipamentos;
- 2.87 Suporte a ativação de filtro de conteúdo por URL com atualização automática da base de dados, por palavra, categorias e no mínimo 40 categorias e filtro por grupos de usuários, que podem ser definidos por:
- 2.87.1 Deve possuir a capacidade de criação de políticas baseadas no controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
- 2.87.2 Deve possuir integração com LDAP para integração de usuários e grupos permitindo o controle/políticas baseadas em usuários e grupos de usuários;
- 2.87.3 Endereços IP;

3. ESPECIFICAÇÃO TÉCNICA GERENCIA CENTRALIZADA, E EMISSÃO DE RELATORIOS:

- 3.1. A solução ofertada deverá ser entregue com hardware, software, licenças, assim como qualquer outro componente necessário a seu pleno funcionamento.
- 3.2. Característica física:
- 3.2.1. Fontes de alimentação hot-plug em redundância (1+1);
- 3.2.2. Possuir capacidade de armazenamento mínima de 900 (Novecentos) Gb
- 3.2.3. Suportar no mínimo 5.000 (cinco mil) logs/flows por segundo.
- 3.2.4. Possuir interfaces de rede Ethernet com as seguintes características:
- 3.2.5. No mínimo 02 (duas) portas RJ-45 1 (um)GbE;
- 3.3. As funcionalidades de gerência e retenção de logs que compõem a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 3.4. Centralizar os logs e relatórios, usando uma única interface de gerenciamento;
- 3.5. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 3.6. O armazenamento poderá ser realizado através de composição com solução de terceiros como por exemplo SIEM (Security Information and Event Management);
- 3.7. Não será permitido a instalação de cliente para administração do appliance de Firewall;

- 3.8. O gerenciamento deve permitir/possuir:
- 3.8.1. Visualização de logs e relatórios relacionados às políticas de firewall e controle de aplicação;
 - 3.8.2. Visualização de logs e relatórios relacionados às IPS, Controle de Aplicação e Anti-Malware;
 - 3.8.3. Visualização de logs e relatórios relacionados às políticas de Filtro de URL;
 - 3.8.4. Monitoração de logs;
 - 3.8.5. Ferramentas de investigação de logs;
 - 3.8.6. Visualização das capturas de pacotes realizadas nos ataques detectados;
 - 3.8.7. Acesso concorrente de administradores;
- 3.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- 3.10. Deve permitir monitorar eventos diretamente relacionados à identificação de aplicação e análise de ameaças como, mas não limitado à ocorrência de botnets, ocorrência de vírus na rede e acesso a sites de grupos extremistas ou pedofilia;
- 3.11. Deve permitir bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- 3.12. Deve permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 3.13. Deve permitir autenticação integrada ao Microsoft Active Directory (AD) e servidor Radius;
- 3.14. Deve possuir geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- 3.15. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo comparar os diferentes consumos realizados pelas aplicações no decorrer do tempo;
- 3.16. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spyware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
- 3.17. Deve permitir a criação de painéis de instrumentos (dashboards) ou relatórios customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, ameaças identificadas pelo malwares detectados, aplicações mais utilizadas, protocolos mais utilizados, principais atacantes (com informação de geolocalização);

- 3.18. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- 3.19. Deve prover uma visualização sumarizada das aplicações e URLs que passaram pela solução;
- 3.20. Deve possuir mecanismo "Drill-Down" para navegação nos dashboards em tempo real;
- 3.21. Deve ser possível exportar os logs em CSV;
- 3.22. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução;
- 3.23. Deve possibilitar a exibição das seguintes informações, de forma histórica em tempo real:
 - 3.23.1. Situação do dispositivo e do cluster;
 - 3.23.2. Principais aplicações;
 - 3.23.3. Principais aplicações por risco;
 - 3.23.4. Principais ameaças;
 - 3.23.5. Uso de CPU e memória;
- 3.24. No mínimo os seguintes relatórios devem ser gerados:
 - 3.24.1. Resumo gráfico de aplicações utilizadas;
 - 3.24.2. Principais aplicações por utilização de largura de banda de entrada e saída;
 - 3.24.3. Principais aplicações por taxa de transferência de bytes;
 - 3.24.4. Principais hosts por número de ameaças identificadas;
 - 3.24.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, ameaças de rede vinculadas a este tráfego;
 - 3.24.6. Deve permitir a criação de relatórios personalizados
- 3.25. O gerenciamento deve permitir/possuir:
 - 3.25.1. Criação e administração de políticas de firewall e controle de aplicação;
 - 3.25.2. Criação e administração de políticas de IPS e Anti-Malware;
 - 3.25.3. Criação e administração de políticas de Filtro de URL;
 - 3.25.4. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
 - 3.25.5. Alerta de alterações, no caso acesso simultâneo de dois ou mais administradores;
 - 3.25.6. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
 - 3.25.7. Autenticação integrada ao Microsoft Active Directory (AD) e servidor Radius;
 - 3.25.8. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;






- 3.25.9. Backup das configurações e rollback de configuração para a última configuração salva;
- 3.25.10. Deve possuir mecanismo de validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras;
- 3.25.11. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

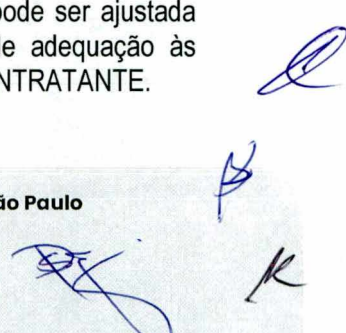
4. Para o Serviço de Suporte Técnico, Manutenção e Garantia:

4.1. Para os equipamentos e softwares que fazem parte do escopo desse edital, a contratada deverá, durante todo o período de garantia, visando a integridade dos produtos e ambiente, realizar o monitoramento contínuo e análise do tráfego e logs visando prevenir, melhorar sua detecção e reduzir tempos de resposta a incidentes de segurança conforme termos a seguir:

- 4.1.1. Os serviços serão prestados vinte quatro (24) horas por dia, sete (7) dias por semana inclusive sábados, domingos e feriados.
- 4.1.2. Os serviços serão prestados em ambiente externo à contratante, sendo o acesso para monitoramento, realizado via VPN a ser disponibilizada pela CONTRATANTE.
- 4.1.3. Os serviços de suporte técnico serão acionados a partir da queda, falha ou registro de indisponibilidade gerado pelo monitoramento (quando for o caso) e/ou por meio de abertura de chamado a critério da equipe técnica da CONTRATANTE. Esses chamados serão classificados conforme as severidades especificadas a seguir:
 - a) Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade na solução ou em qualquer serviço que a compõe; para a criação/configuração de políticas nos firewalls; para aplicação de ações de respostas a ataque. Prazo para início do atendimento: 1 horas.
 - b) Severidade MÉDIA: Esse nível de severidade é aplicado para solicitações de criação/configuração de políticas nos demais serviços que compõem a solução; quando há problema, simultâneo ou não, nos elementos que compõem os serviços/solução, embora ainda estejam disponíveis. Prazo para início do atendimento: 2 horas.
 - c) Severidade BAIXA: Esse nível de severidade é aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados. Prazo para início do atendimento: 6 horas.
- 4.1.4. Faculta-se à CONTRATADA substituir temporariamente o equipamento, peça e componente defeituoso por outros de mesmas características técnicas, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva.

- 4.1.5. O prazo máximo para a substituição temporária será de 30 (trinta) dias, sendo que neste prazo o equipamento, peça e componente substituído deverá ser devolvido ao CONTRATANTE em pleno estado de funcionamento ou ser substituído definitivamente.
- 4.1.6. A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer equipamento, peça e componente que venha a se enquadrar em, pelo menos, um dos seguintes casos:
- a) Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;
 - b) Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;
 - c) No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se à CONTRATADA promover a sua substituição em caráter definitivo;
 - d) A substituição definitiva será admitida com anuência do CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, peça e componente ofertado, em relação àquele que está sendo substituído.
- 4.1.7. A CONTRATADA tornará disponíveis informações sobre desempenho e falhas (indisponibilidade) da solução de forma interativa ("on-line"), a partir do início da operação em produção).
- 4.1.8. Quando da ocorrência de falhas que tornem o serviço/solução indisponível por mais de 1 (uma) hora, a CONTRATADA deverá entregar ao CONTRATANTE, juntamente com o relatório técnico mensal, a descrição detalhada da ocorrência, suas causas e as ações corretivas realizadas para tornar o serviço/solução novamente disponível.
- 4.1.9. A CONTRATADA deverá manter registro dos eventos, que porventura tenham provocado interrupções na solução dentro do período do faturamento mensal, de modo a justificar ao CONTRATANTE a não consideração de tempos de inoperância, causados por falta de energia elétrica nas dependências do CONTRATANTE, por ações ou solicitações do CONTRATANTE ou ainda por manutenções programadas.
- 4.1.10. A CONTRATADA somente poderá efetuar manutenção técnica na solução e seus componentes após aprovação por parte do CONTRATANTE. Caso a manutenção seja efetuada sem essa aprovação, será considerado como indisponibilidade.
- 4.1.11. Será considerado o Prazo de Solução Definitiva como o tempo decorrido entre o registro de um chamado e a solução definitiva para efeito dos níveis exigidos.

- 4.1.12. Os chamados de severidade ALTA poderão ser atendidos on-site, a critério do CONTRATANTE. É vedado a CONTRATADA interromper o atendimento até que o serviço seja efetivamente recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. A interrupção do suporte técnico de um chamado desse tipo de severidade por parte da CONTRATADA e que não tenha sido previamente autorizado pelo CONTRATANTE, poderá ensejar em aplicação de penalidades previstas.
- 4.1.13. Após concluído o suporte técnico e com o serviço efetivamente recolocado em pleno estado de funcionamento, a CONTRATADA comunicará o fato à equipe técnica do CONTRATANTE e solicitará autorização para o fechamento do chamado. Caso o CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até o momento em que o serviço seja efetivamente recolocado em pleno estado de funcionamento pela CONTRATADA. Nesse caso, o CONTRATANTE fornecerá por e-mail, telefone ou através da interface de gerenciamento as pendências relativas ao chamado aberto.
- 4.1.14. Caso não haja manifestação dentro do prazo estipulado para o chamado em questão ou caso o CONTRATANTE entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.
- 4.1.15. O CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal de usuários que terão login e senha com perfis de acessos adequados aos serviços que compõem a solução bem como para abrir chamados e administrar todo ambiente. Esses perfis serão criados a critério do CONTRATANTE e configurados inicialmente pela CONTRATADA.
- 4.1.16. Ao detectar tentativas de ataques à rede interna do CONTRATANTE ou aos serviços disponíveis em seu ambiente, a CONTRATADA deverá adotar, de imediato, as medidas de combate ao ataque independentemente das que forem estabelecidas pelo CONTRATANTE. No caso dessas medidas implicarem interrupções e/ou descaracterização dos serviços em uso, a CONTRATADA deverá entrar em contato com o CONTRATANTE em, no máximo, 15 (quinze) minutos, para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las. O CONTRATANTE se responsabilizará por eventuais danos causados pela não autorização de ações recomendadas pela CONTRATADA.
- 4.1.17. A lista de usuários da CONTRATANTE (login/Admin) pode ser ajustada durante o período de vigência do contrato a título de adequação às necessidades do CONTRATANTE, sem ônus para o CONTRATANTE.





CO-17.12/2025

- 4.1.18. Todas as configurações de regras após a entrega e aceite da solução serão realizadas pela CONTRATANTE, exceto quando aberto chamado previsto no item 4.1.3 e incidentes de segurança detectados pela CONTRATADA.
- 4.1.19. Pelo não cumprimento do índice mínimo de 99,95% DISPONIBILIDADE previsto, serão aplicadas as penalidades previstas em Contrato.
- 4.1.20. Durante todo o período contratual estará incorporado o serviço de manutenção, garantia e suporte de toda solução entregue.

5. A CONTRATADA obriga-se a:

- 5.1. A Contratada deverá oferecer garantia, suporte e licenças dos equipamentos e suas funcionalidades contratadas por um prazo 180 (cento e oitenta) dias, a contar da data de sua efetiva instalação; durante o período de cobertura, a CONTRATADA deverá prestar Serviços de Manutenção "On Site", para todos os componentes do objeto deste edital, incluindo configuração técnica do produto;
- 5.2. Disponibilizar profissionais certificados pelos fabricantes da solução de NGFW e nas melhores práticas de gestão de TI, conforme abaixo:
 - 5.2.1. Profissional certificado ITIL V3 ou superior;
 - 5.2.2. Profissional certificado Cobit;
 - 5.2.3. Profissional certificado PMP;
 - 5.2.4. Profissional certificado PMO CP;
 - 5.2.5. Profissional certificado CompTIA CySA+;
 - 5.2.6. Dois profissionais certificados no produto de NGFW, com o nível de certificação Profissional ou superior;
- 5.3. Instalar, configurar e acompanhar os testes de funcionamento antes da entrada de produção dos equipamentos;
- 5.4. Orientar tecnicamente os responsáveis pela operação dos equipamentos, fornecendo os esclarecimentos necessários ao seu perfeito funcionamento;
- 5.5. Disponibilizar número de telefone (local ou DDG) para suporte telefônico (24x7x365) e abertura de chamados técnicos;
- 5.6. Proceder à entrega dos equipamentos, devidamente embalados, de forma a não serem danificados durante a operação de transporte e de carga e descarga, com as especificações detalhadas para conferência;
- 5.7. O modelo do equipamento ofertado deverá estar em linha normal de produção e sem previsão de encerramento;

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

Rua Libero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP



- 5.8. O tempo máximo de atendimento para os chamados de defeitos deverá ser de 4 hs (quatro horas) e de solução em até 6 h (seis horas) a contar do registro de abertura do chamado no Centro de Atendimento Técnico da Contratada, realizando testes e corrigir defeitos, inclusive com a sua substituição quando necessário, sem ônus para a CONTRATANTE, durante o período de garantia;
- 5.9. A cada visita técnica realizada nas dependências da CONTRATANTE a CONTRATADA deverá emitir um relatório de execução das atividades, relacionando os serviços executados e lista de equipamentos que eventualmente sejam deixados ou retirados das dependências da CONTRATANTE;
- 5.10. Caso a Contratada não consiga recuperar o equipamento em até 72 horas após a abertura do chamado, o appliance com problema deverá ser substituído por outro novo.
- 5.11. A Contratada deverá acompanhar com pessoal in loco o primeiro dia útil de operação do ambiente em produção.

6. QUANTIDADE:

ITEM	DESCRIÇÃO	QUANT.	UNID.
01	FIREWALL NEXT GENERATION (NGFW)	2	UN
02	Pacotes de Licenças IPS / GATEWAY Anti-Malware e Licenças de Alta disponibilidade HA (High-Availability)	6	Meses
03	Suporte técnico, manutenção e garantia	6	Meses
04	Gerencia Centralizada e emissão de relatórios	2	UN

7. CONFIDENCIALIDADE

- 7.1 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;



- 7.2 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.

8. ACEITE / INSTALAÇÃO DAS LICENÇAS

- 8.1. As licenças deverão ser instaladas até dia 22/12/2025 e deverão estar validas e disponíveis para uso a partir 23/12/2025;
- 8.2. Após a disponibilização das licenças para uso, a equipe técnica da PRODAM emitirá o "TERMO DE ACEITE" em até 5 dias uteis.

9. PENALIDADES

- 9.1. Será aplicado multa de 1% (um por cento) por dia de atraso na disponibilização de uso das licenças, sob o valor do contrato;
- 9.2. Caso o tempo para atendimento ultrapasse as 4 horas, contadas a partir da abertura do chamado, conforme item 5.8, haverá multa de 1% por hora de atraso, calculado sobre o valor mensal do contrato;
- 9.3. Caso o tempo para atendimento para chamado de severidade alta ultrapasse 1 horas para início do atendimento, contadas a partir da abertura do chamado, haverá multa de 1% por hora de atraso, calculado sobre o valor mensal do contrato;
- 9.4. Caso o tempo para atendimento para chamado de severidade média e baixa ultrapasse respectivamente 2 e 6 horas para início do atendimento, contadas a partir da abertura do chamado, haverá multa de 1% por hora de atraso, calculado sobre o valor mensal do contrato;
- 9.5. Caso o tempo para a solução de um chamado de manutenção ultrapasse as 6 horas, contadas a partir da abertura do chamado, conforme item 5.8, haverá multa de 0,5% por hora de atraso, calculado sobre o valor mensal do contrato;
- 9.6. Caso haja atraso na substituição do equipamento avariado por um novo após 120 horas da abertura do chamado sem solução, conforme item 5.10, será cobrada multa de 5% por dia de atraso, calculado sobre o valor do contrato.
- 9.7. Caso haja descumprimento do SLA, será previsto multa de 5% do valor mensal do contrato.



CO-17.12/2025

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 **TELETIX COMPUTADORES E SISTEMAS LTDA.**, sediada em São Paulo/SP, na Avenida Doutor Cardoso de Melo nº 1308, Sala 71, bairro Vila Olímpia, CNPJ nº 79.345.583/0010-33, doravante denominada CONTRATADA;

Considerando que, em razão do Contrato n.º 17.12/2025 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.

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

Rua Líbero Badaró, 425 – Centro – CEP: 01009-905 – São Paulo – SP



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.





CO-17.12/2025

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.

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

Rua Líbero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP





CO-17.12/2025

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;

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

Rua Líbero Badaró, 425 – Centro – CEP: 01009-905 – São Paulo – SP





CO-17.12/2025

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.

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

Rua Líbero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP





CO-17.12/2025

ANEXO III

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

Nome da empresa: **TELETEX COMPUTADORES E SISTEMAS LTDA**

CNPJ nº: 79.345.583/0010-33

Número do contrato: CO-17.12/2025

Vigência contratual: 180 (cento e oitenta) dias

Objeto contratual: **FORNECIMENTO DE SERVIÇO PARA SOLUÇÕES DE SEGURANÇA COMPOSTA DE FIREWALL PARA PROVER SEGURANÇA E PROTEÇÃO DE REDES**

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), responsabilizando-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.

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

Rua Líbero Badaró, 425 - Centro - CEP: 01009-905 - São Paulo - SP



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

empenho não utilizado.III - Designo os seguintes Fiscais de Contrato: Bruno Correa Falcão Oliveira, RF: 837.660.3 e Janos Zimmerhansl Junior, RF: 840.090.3, para atuarem em conjunto ou individualmente na fiscalização da execução contratual.IV - Publique-se.

Arquivo (Número do documento SEI)

[151164613](#)

Despacho autorizatório (NP) | Documento: [151213234](#)

DADOS DA LICITAÇÃO

Número da Ata

868/2025 - SMS.G

Natureza

Materiais e equipamentos

Descrição da natureza

material médico hospitalar

Objeto da licitação

fornecimento de 600 envelopes de fio cirúrgico, poliglecaprone, incolor, 4-0, absorvível, monofilamentar, 70 cm, agulha 3/8 circulo, triangular, 1,9 cm

Processo

6210.2026/0001269-4

Local de execução

São Paulo - SP

Data da Publicação

18/02/2026

Texto do despacho

PROCESSO SEI Nº 6210.2026/0001269-4 I - À vista dos elementos constantes nos autos deste processo administrativo, considerando que nele consta parecer da Assessoria Jurídica, opinando quanto a regularidade do procedimento, com fundamento no artigo 40, II, da Lei Federal nº 14.133/21, no artigo 101 do Decreto Municipal nº 62.100/22 e a competência que me foi delegada pela Portaria nº 12/2025 - HSPM, publicada no D.O.C. de 28 de março de 2025, AUTORIZO a utilização da Ata de Registro de Preços nº 868/2025 - SMS.G, da qual o HSPM é órgão participante, e a contratação da detentora BIOLINE FIOS CIRÚRGICOS LTDA, CNPJ: 37.844.479/0002-33, para o fornecimento de 600 envelopes de fio cirúrgico, poliglecaprone, incolor, 4-0, absorvível, monofilamentar, 70 cm, agulha 3/8 circulo, triangular, 1,9 cm, no valor unitário de R\$ 8,16 e valor total de R\$ 4.896,00 (quatro mil, oitocentos e noventa e seis reais). Prazo de Realização da Despesa: 10 (dez) dias úteis a contar da emissão da Ordem de Fornecimento. Os preços estão compatíveis com a pesquisa de mercado juntada nos autos, cuja despesa será suportada pela dotação orçamentária 02.10.302.4016.2.507.3.3.90.30.00, conforme Nota

de Reserva nº 631/2026.II - Autorizo ainda, a emissão da Nota de Empenho no respectivo valor, bem como o cancelamento de eventual saldo de empenho não utilizado.III - Designo os seguintes Fiscais de Contrato: Bruno Correa Falcão Oliveira, RF: 837.660.3 e Janos Zimmerhansl Junior, RF: 840.090.3, para atuarem em conjunto ou individualmente na fiscalização da execução contratual.IV - Publique-se.

Arquivo (Número do documento SEI)

[151163805](#)

Agência Reguladora de Serviços Públicos do Município de São Paulo

GESTÃO DE CONTRATOS

Extrato de Aditamento (NP) | Documento: [150828360](#)

PRINCIPAL

Número do Contrato

0042025

Contratado(a)

SAKURA DEDETIZADORA LTDA

Tipo de Pessoa

Jurídica

CPF /CNPJ/ RNE

14340628000140

Data da Assinatura

06/02/2026

Prazo do Contrato

12

Tipo do Prazo

Mês

Síntese (Texto do Despacho)

CLÁUSULA 1ª Fica prorrogado o prazo de vigência do Contrato nº 004/SPREGULA/2025, por mais 12 (doze) mês, a partir de 11/02/2026, no valor total de R\$ 5.177,88 (Cinco mil cento e setenta e sete reais e oitenta e oito centavos).CLÁUSULA 2ª Ficam ratificadas todas as cláusulas e condições do Contrato oraaditado, no que não contraditem o presente Termo de Aditamento.E, por estar assim de acordo, assinam o presente em formato digital, para que produzam seus efeitos legais.

Data de Publicação

18/02/2026

Íntegra do Contrato (Número do Documento SEI)

[150708543](#)

Extrato de Contrato/Nota de empenho (NP) | Documento: [151242161](#)

PRINCIPAL

Número do Contrato

0142025

Contratado(a)

HEBROM CONSTRUCOES LTDA.

Tipo de Pessoa

Jurídica

CPF /CNPJ/ RNE

04.941.945/0001-69

Data da Assinatura

08/10/2025

Prazo do Contrato

120

Tipo do Prazo

Dia

Síntese (Texto do Despacho)

Termo de Apostilamento que tem como objeto a prorrogação da execução contratual (art. 111, caput, c.c. art. 115, §6º, todos da Lei Federal nº 14.133/2021).

Data de Publicação

18/02/2026

Íntegra do Contrato (Número do Documento SEI)

[151241958](#)

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

GERÊNCIA JURÍDICA

Extrato de Contrato/Nota de empenho (NP) | Documento: [151165127](#)

PRINCIPAL

Número do Contrato

CO-17.12/2025

Contratado(a)

TELETEX COMPUTADORES E SISTEMAS LTDA

Tipo de Pessoa

Jurídica

CPF /CNPJ/ RNE



79.345.583/0010-33

Data da Assinatura

22/12/2025

Prazo do Contrato

180

Tipo do Prazo

Dia

Síntese (Texto do Despacho)

EXTRATO DE TERMO DE CONTRATO. CONTRATO Nº CO-17.12/2025. PROCESSO SEI Nº 7010.2025/0011399-0. DISPENSA DE LICITAÇÃO Nº 12.018/2025, COM FULCRO NO ARTIGO 29, INCISO XV, DA LEI Nº 13.303/16. CONTRATANTE: EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO - PRODAM-SP S/A. CONTRATADA: TELETEX COMPUTADORES E SISTEMAS LTDA (CNPJ: 79.345.583/0010-33). OBJETO: FORNECIMENTO DE SERVIÇO PARA SOLUÇÕES DE SEGURANÇA COMPOSTA DE FIREWALL PARA PROVER SEGURANÇA E PROTEÇÃO DE REDES. VIGÊNCIA: 180 (CENTO E OITENTA) DIAS, CONTADOS A PARTIR DA DATA DE 23 DE DEZEMBRO DE 2025. VALOR: O VALOR TOTAL DO PRESENTE CONTRATO É DE R\$ 446.227,56 (QUATROCENTOS E QUARENTA E SEIS MIL, DUZENTOS E VINTE E SETE REAIS E CINQUENTA E SEIS CENTAVOS).

Data de Publicação

18/02/2026

Íntegra do Contrato (Número do Documento SEI)

[151163158](#)

São Paulo Turismo

COMISSÃO PERMANENTE DE LICITAÇÕES

Prejudicada (NP) | Documento: [151149249](#)

PRINCIPAL

Síntese (Texto do Despacho)

Comunicamos que em 12/02/2026, o Diretor de Gestão e de Relação com Investidores FRACASSOU o PREGÃO ELETRÔNICO nº. 041/25 inserido no sistema Licitações-e sob o número 1085285, após desclassificação motivada de todos os licitantes.

Anexo I (Número do Documento SEI)

[151086464](#)

Data de Publicação

13/02/2026

Companhia de Engenharia de Tráfego

DEPARTAMENTO DE AQUISIÇÃO DE BENS E SERVIÇOS ESPECIALIZADOS

Outras (NP) | Documento: [151219623](#)

PRINCIPAL

Especificação de Outras

Esclarecimento 03 - PGERP 006/2025 - OBRAS CIVIS

Síntese (Texto do Despacho)

EXPEDIENTE Nº 0759/24 LICITAÇÃO PREGÃO ELETRÔNICO Nº 006/2025 REGISTRO DE PREÇOS PARA PRESTAÇÃO DE SERVIÇOS DE PEQUENAS OBRAS CIVIS DE SINALIZAÇÃO VIARIA NAS VIAS PÚBLICAS DO MUNICÍPIO DE SÃO PAULO, COM FORNECIMENTO DE MATERIAIS. ESCLARECIMENTO Nº 03 Perguntas: Ao se comparar a relação de equipamentos mínimos indicada na declaração com os equipamentos considerados nas composições de preços dos serviços, persistem divergências relevantes quanto às especificações técnicas, capacidades operacionais e tipologia dos equipamentos envolvidos, circunstância que pode gerar interpretações distintas no momento da diligência e comprometer a segurança jurídica do certame. Dessa forma, solicitamos, respeitosamente, esclarecer: 1) Se a diligência considerará exclusivamente a relação mínima de equipamentos prevista na declaração de disponibilidade mínima de veículos e equipamentos sem considerar especificações técnicas; 2) Quais características técnicas mínimas serão adotadas pela área técnica da CET para caracterizar os equipamentos como adequados à execução dos serviços, especialmente quanto à capacidade operacional dos caminhões basculantes, rolos compactadores e compressores; 3) Se serão adotadas como referência as especificações dos equipamentos utilizados nas composições de preços dos serviços. O presente esclarecimento é essencial para o adequado planejamento operacional da empresa e para a correta formulação da proposta, evitando interpretações divergentes das exigências editalícias. Respostas: Senhores, Em atenção à e-mail de empresa interessada em participar do Pregão Eletrônico em referência, consultamos a área técnica e temos a informar o que segue: 1) - Sim, conforme o relacionado no item 14.4 do Anexo II - Termo de Referência do Edital. 2) - As especificações dos equipamentos listados no item 14.4 devem atender às atividades descritas no item 7, ambos do Anexo II - Termo de Referência do Edital, sendo que a escolha desses equipamentos deve ser compatível com os serviços, o planejamento da Contratada e adequada ao mesmo anexo II. 3) - Não. GSP,12/02/26, Gerente de Suprimentos

Data de Publicação

16/02/26

Comunicado (NP) | Documento: [151237540](#)

PRINCIPAL

Síntese (Texto do Despacho)

EXPEDIENTE Nº 0144/2025 MODALIDADE: PREGÃO ELETRÔNICO Nº 001/26 CONTRATAÇÃO DE SERVIÇOS SECURITÁRIOS DE VIDA EM GRUPO A EMPREGADOS DA COMPANHIA DE ENGENHARIA DE TRÁFEGO - CET ESCLARECIMENTO Nº 10 PERGUNTA 01 A resposta 08 do Esclarecimento nº 2 informa os prêmios mensais pagos à companhia Sura de JAN/23 a DEZ/25. Porém, a relação de sinistros indenizados, Anexo D do edital, foi limitada aos processos ocorridos até 2/MAI/25. Solicitamos, assim, a complementação das informações referentes aos processos de sinistro avisados entre MAI/25 a DEZ/25, para a correta equivalência desses dados com os prêmios auferidos no mesmo período. RESPOSTA PERGUNTA 01 DATA SINISTRO E VALOR DA INDENIZAÇÃO 13/06/2025 R\$ 90.039,60 18/06/2025 R\$60.448,50 23/06/2025 R\$ 100.299,00 22/07/2025 R\$184.439,56 21/09/2025 R\$189.972,60 05/10/2025 R\$76.777,08 13/10/2025 R\$105.634,95 24/10/2025 R\$117.671,25 28/10/2025 R\$75.988,35 28/10/2025 R\$90.734,55 10/12/2025 R\$178.060,05 Gerência de Suprimentos

Data de Publicação

16/02/2026

DEPARTAMENTODE AQUISIÇÕES DE BENS E SERVIÇOS PADRONIZADOS

Despacho autorizatório (NP) | Documento: [151186555](#)

DADOS DA LICITAÇÃO

Número

06/2026

Cotação Eletrônica

Sim

Natureza

Selecionar

Descrição da natureza

IMPRESSOS PADRONIZADOS

Objeto da licitação

FORNECIMENTO E CONFECÇÃO DE 1.000 CARDENETAS COM CANETA - CET 50 ANOS.

Processo

7410.2026/0000454-3

Local de execução

São Paulo - SP

Data da Publicação