



**Governo do Estado de São Paulo
Fundação de Previdência Complementar do Estado de São Paulo
PREVCOM-AUD-Auditoria Interna**

TERMO DE REFERÊNCIA

Nº do Processo: 271.00000630/2026-50

Interessado: Presidência, Gabinete da Presidência, Diretoria Administrativa, Contratos e Licitações

Assunto: Auditoria Especializada

TERMO DE REFERÊNCIA PREVCOM Nº 037/2026

1. OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. O objeto do presente Termo de Referência é a contratação de empresa especializada para prestação de serviços técnicos de Teste de Intrusão (Pentest), com o objetivo de identificar vulnerabilidades, avaliar a efetividade dos controles de segurança da informação e verificar o nível de exposição dos ativos tecnológicos da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM, mediante execução controlada de testes de segurança e emissão de relatórios de auditoria contendo evidências e recomendações para mitigação dos riscos identificados.

1.2. A contratação compreenderá 1 (uma) auditoria técnica especializada em Pentest, incluindo a realização de reteste para validação das correções implementadas pela CONTRATANTE, constituindo ambos parte integrante do objeto contratado. A vigência do contrato será de 4 (quatro) meses, contados da assinatura do instrumento contratual, podendo ser prorrogada, nos termos da Lei nº 14.133/2021, exclusivamente para conclusão do objeto, caso devidamente justificado.

1.3. O objeto desta contratação não se enquadra como serviço de luxo, em observância ao Decreto Estadual nº 67.985, de 27 de setembro de 2023.

1.4. A contratação será formalizada por meio de instrumento contratual ou documento equivalente, como contratação direta com fundamento no Art. 75, inciso II, da Lei nº 14.133, de 2021.

1.5. Não será admitida a subcontratação total ou parcial do objeto sem prévia autorização da CONTRATANTE.

1.6. Os serviços deverão ser prestados conforme as condições, especificações e exigências estabelecidas neste Termo de Referência.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A crescente exposição aos riscos cibernéticos, associada à elevada dependência dos processos institucionais em relação aos recursos tecnológicos, impõe a necessidade de avaliação periódica da efetividade dos controles de segurança da informação adotados pela Fundação.

2.2. Com base na exposição crescente da Fundação aos riscos cibernéticos e ao objetivo de

avaliação neste cenário, torna-se necessária a contratação de empresa especializada para realização de auditoria técnica e especializada em Pentest, com atuação independente e utilização de metodologias reconhecidas internacionalmente, visando identificar vulnerabilidades técnicas eventualmente existentes nos ativos tecnológicos da PREVCOM, bem como avaliar a possibilidade de exploração dessas fragilidades por agentes maliciosos.

2.3 Os resultados obtidos subsidiarão a adoção de medidas corretivas e preventivas destinadas ao fortalecimento da segurança da informação, cibernética, da gestão de riscos e da proteção das informações institucionais, em alinhamento às melhores práticas de mercado e às exigências regulatórias aplicáveis.

3. DESCRIÇÃO DA SOLUÇÃO E ESCOPO DOS SERVIÇOS

3.1. A CONTRATADA deverá executar a auditoria especializada em Pentest utilizando metodologia estruturada e reconhecida internacionalmente, contemplando, no mínimo:

a) Planejamento e preparação

- reunião de kick-off;
- alinhamento do cronograma x escopo;
- alinhamento dos procedimentos de comunicação.

b) Reconhecimento e mapeamento

- levantamento da superfície de ataque;
- identificação dos ativos objeto dos testes;
- enumeração de serviços e aplicações.

c) Execução dos testes

- identificação de vulnerabilidades;
- exploração controlada das fragilidades identificadas;
- validação da possibilidade de comprometimento dos ativos;
- testes manuais e automatizados.

d) Análise dos resultados

- classificação das vulnerabilidades por criticidade;
- identificação dos riscos associados;
- consolidação das evidências obtidas.

e) Emissão dos relatórios

- relatório executivo de auditoria;
- relatório de auditoria técnica;
- recomendações de correção.

f) Reunião sobre os resultados obtidos

- apresentação executiva;
- esclarecimento técnico das vulnerabilidades identificadas.

g) Reteste

- validação das correções implementadas pela Contratante;
- emissão do Relatório de Auditoria do Reteste.

3.2. Para fins deste Termo de Referência, entende-se a necessidade pelos trabalhos de

auditoria baseados em Teste de Intrusão cibernética (conhecido como *pentest* ou teste de penetração), que é uma simulação autorizada de um ciberataque. Ele é realizado por especialistas em segurança da informação (hackers éticos) para avaliar a segurança de sistemas, redes e aplicativos, descobrindo e explorando vulnerabilidades antes que criminosos o façam

3.3. Estima-se a realização de até 2 (duas) demandas de penetração durante o período contratual de 4 (quatro) meses, tratando-se de quantitativo meramente referencial designado para o pentest e reteste, integrando o mesmo objeto.

3.4. Os serviços deverão resultar na entrega de relatório de auditoria técnica conclusiva, contendo, no mínimo:

- I. delimitação do escopo da análise;
- II. descrição da metodologia adotada;
- III. relação das fontes de informação consultadas;
- IV. descrição dos achados relevantes;
- V. identificação e classificação dos riscos e contingências (baixo, médio ou alto);
- VI. matriz de riscos consolidada, com indicação de probabilidade e impacto;
- VII. recomendações técnicas para mitigação dos riscos identificados;
- VIII. conclusão técnica consolidada;
- IX. resumo executivo, contendo síntese dos principais riscos e recomendações, em linguagem acessível à alta gestão.

3.5. Após a entrega do Relatório de Auditoria Técnica, a CONTRATANTE poderá solicitar a realização do reteste das vulnerabilidades identificadas, mediante comunicação formal informando a implementação das correções, observado o prazo máximo de 45 (quarenta e cinco) dias contados do recebimento do relatório de auditoria.

3.5.1. O reteste constitui etapa obrigatória desta contratação, não implicando qualquer custo adicional ao CONTRATANTE.

3.5.2. Recebida a solicitação, a CONTRATADA deverá realizar o reteste e apresentar o respectivo Relatório de Auditoria de Reteste no prazo máximo de 10 (dez) dias úteis.

3.5.3. O Relatório de Auditoria de Reteste deverá conter, no mínimo:

- I. situação atualizada de cada vulnerabilidade identificada;
- II. evidências técnicas da validação realizada;
- III. indicação das vulnerabilidades corrigidas, parcialmente corrigidas, remanescentes ou aceitas pelo CONTRATANTE;
- IV. classificação atualizada dos riscos, utilizando a metodologia CVSS (*Common Vulnerability Scoring System*) vigente.

3.5.4. Caso seja constatado que determinada vulnerabilidade permaneceu em razão de inconsistência técnica nas recomendações originalmente emitidas pela CONTRATADA, esta deverá complementar as orientações e realizar nova validação específica, sem custos adicionais ao CONTRATANTE, sem prejuízo da aplicação das sanções previstas no contrato, quando cabíveis.

3.6. Os serviços deverão ser executados com observância dos princípios de confidencialidade, independência técnica, imparcialidade e rastreabilidade das análises realizadas.

4. ESCOPO DOS TESTES

4.1 Os serviços deverão contemplar, conforme autorizado pela CONTRATANTE:

- Aplicações Web: Portal do Participante; Área Restrita; demais aplicações expostas à internet.
- Infraestrutura Externa: endereços IP públicos; firewall; serviços publicados.
- Infraestrutura Interna: servidores; rede interna e serviços críticos.
- Ambiente de Autenticação: *Active Directory*; mecanismos de autenticação e privilégios e acessos.

4.2. A relação definitiva dos ativos será fornecida pela CONTRATANTE antes do início da execução dos serviços.

4.3. A contratada deverá comprovar experiência na execução de serviços na realização de *pentest*, auditoria ou atividades correlatas, mediante a apresentação de, no mínimo, 2 (dois) atestados de capacidade técnica, emitidos por pessoas jurídicas de direito público ou privado, referentes a serviços realizados nos últimos 5 (cinco) anos.

4.3.1. Consideram-se compatíveis os serviços de *Pentest*, Avaliação de Vulnerabilidades, *Red Team*, Auditoria de Segurança da Informação ou outros serviços equivalentes relacionados à identificação e exploração controlada de vulnerabilidades em ativos tecnológicos.

4.3.2. Para fins de comprovação, os atestados deverão conter, no mínimo:

- I. identificação da pessoa jurídica contratante;
- II. descrição do objeto contratado, com detalhamento suficiente para aferição da compatibilidade com o objeto deste Termo de Referência;
- III. período de execução dos serviços;
- IV. declaração de que os serviços foram executados de forma satisfatória;
- V. identificação e meio de contato do emitente.

4.3.3. Será admitido o somatório de atestados para fins de comprovação da experiência exigida.

4.3.4. A Contratante poderá realizar diligências para verificar a veracidade das informações constantes dos atestados apresentados, inclusive mediante contato com os emitentes.

4.4. A contratada deverá dispor de equipe técnica qualificada, com formação e experiência compatíveis com a natureza dos serviços.

4.4.1. Para fins de comprovação da qualificação da equipe técnica, deverão ser apresentados:

- I. relação nominal dos profissionais indicados para execução dos serviços;
- II. currículos profissionais atualizados;
- III. documentos comprobatórios da formação acadêmica;
- IV. comprovação de vínculo profissional com a contratada, por meio de contrato social, registro em carteira, contrato de prestação de serviços ou documento equivalente.

4.4.2. A experiência profissional informada nos currículos poderá ser objeto de diligência pela Contratante, mediante solicitação de documentos complementares.

4.5. A contratada deverá assegurar que os profissionais alocados na execução dos serviços possuam capacidade técnica compatível com a complexidade das demandas.

4.5.1. A Contratante poderá, mediante justificativa, solicitar a substituição de profissionais que não apresentem desempenho satisfatório ou não atendam aos requisitos estabelecidos neste Termo de Referência.

4.6. A execução dos serviços deverá observar, obrigatoriamente, os seguintes princípios:

- I. confidencialidade das informações;

- II. independência técnica;
- III. imparcialidade;
- IV. rastreabilidade das análises realizadas;
- V. consistência técnica das conclusões apresentadas.

4.6.1. Para fins de comprovação do atendimento aos princípios estabelecidos, a contratada deverá apresentar, previamente à assinatura do contrato:

- I. declaração formal de confidencialidade e inexistência de conflito de interesses;
- II. descrição dos procedimentos adotados para garantia do sigilo e da integridade das informações.

4.7. A contratada deverá comunicar previamente à Contratante a existência de qualquer situação que possa caracterizar conflito de interesses, cabendo à Contratante deliberar sobre a continuidade da execução contratual ou a necessidade de substituição da equipe envolvida.

5. REQUISITOS DA CONTRATADA

5.1. A empresa deverá possuir experiência comprovada na prestação de serviços de auditoria especializada em Testes de Intrusão; manter equipe técnica especializada; garantir a confidencialidade das informações acessadas; responsabilizar-se integralmente por eventuais danos decorrentes da execução inadequada dos serviços e possuir profissionais com certificações ou qualificações compatíveis, sendo desejáveis: OSCP; CEH; CompTIA PenTest+; CISSP; Security+.

5.2 A avaliação técnica da proponente observará os critérios estabelecidos no item 8 deste Termo de Referência.

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato será executado pelas partes em conformidade com as condições estabelecidas neste Termo de Referência, respondendo cada uma pelas consequências de eventual inadimplemento.

6.2. Antes do início da execução dos serviços, a CONTRATADA deverá assegurar que todos os profissionais envolvidos assinem Acordo de Confidencialidade (Non-Disclosure Agreement – NDA), comprometendo-se a preservar o sigilo das informações, credenciais, evidências, configurações e demais dados obtidos durante a execução do objeto.

6.3. A CONTRATADA deverá indicar formalmente preposto responsável pela execução dos serviços e pelo relacionamento com o CONTRATANTE durante toda a vigência contratual.

6.4. A execução do contrato será acompanhada e fiscalizada por representante(s) designado(s) pelo CONTRATANTE, competindo-lhe verificar o cumprimento das obrigações contratuais, registrar eventuais ocorrências e atestar o recebimento dos serviços.

6.5. O CONTRATANTE poderá solicitar esclarecimentos, promover reuniões de acompanhamento e determinar a adoção de medidas corretivas necessárias ao adequado cumprimento do objeto contratual.

6.6. O gestor do contrato será responsável pela coordenação da execução contratual, pelo acompanhamento das providências administrativas necessárias e pelo encaminhamento do processo para recebimento definitivo e pagamento.

6.7. A fiscalização exercida pelo CONTRATANTE não exclui nem reduz a responsabilidade da CONTRATADA pela correta execução do objeto contratado.

7. CRITÉRIOS DE MEDIÇÃO, RECEBIMENTO E PAGAMENTO

7.1. A execução do objeto será aferida mediante a entrega dos produtos previstos neste Termo de Referência e a verificação do atendimento integral aos requisitos técnicos estabelecidos para os serviços de *Pentest* e Reteste. Consideram-se produtos mínimos da contratação:

- Plano de Execução dos Trabalhos;
- Relatório Executivo de Auditoria;
- Relatório de Auditoria Técnica contendo as vulnerabilidades identificadas no processo de auditoria, respectivas evidências, classificação de criticidade, pontuação CVSS e recomendações de tratamento;
- Apresentação executiva dos resultados;
- Relatório de Auditoria de Reteste, quando solicitado pela CONTRATANTE, observado o disposto no item 3.5.

7.2. A entrega dos produtos será analisada pelo gestor e pelo fiscal do contrato, que verificarão sua conformidade com o escopo contratado. Caso sejam identificadas inconsistências ou pendências, a CONTRATADA será notificada para promover os ajustes necessários no prazo estabelecido pela fiscalização.

7.3. Após a aprovação dos produtos entregues, será emitido o Termo de Recebimento Definitivo, caracterizando o aceite dos serviços. O recebimento definitivo não afasta a responsabilidade da CONTRATADA quanto à qualidade técnica dos serviços executados.

7.4. O pagamento será efetuado em parcela única, após:

- emissão do Termo de Recebimento Definitivo;
- apresentação da Nota Fiscal;
- comprovação da regularidade fiscal da CONTRATADA.

7.5. O pagamento será realizado mediante crédito em conta bancária indicada pela CONTRATADA, observado o prazo previsto nas normas internas da CONTRATANTE.

8. CRITÉRIOS PARA ESCOLHA DA PROPOSTA MAIS VANTAJOSA E REGIME DE EXECUÇÃO

8.1. A escolha da proposta mais vantajosa observará critérios técnicos e econômicos, considerando a natureza de auditoria especializada na realização de *Pentest* e Reteste. A avaliação priorizará a experiência da proponente, a qualificação da equipe técnica, a metodologia de execução, os controles de segurança da informação e o valor global da proposta, de forma a assegurar a contratação da solução mais adequada às necessidades da CONTRATANTE. Considerando que a qualidade técnica da execução é fator determinante para a confiabilidade dos resultados da auditoria, para a adequada identificação das vulnerabilidades e para a efetividade das recomendações de tratamento, a avaliação técnica terá predominância sobre a avaliação econômica.

8.2. A avaliação técnica terá pontuação máxima de **100 (cem) pontos**, observando-se a seguinte distribuição:

Critério de Avaliação	Pontuação Máxima
Qualificação da equipe técnica	35 pontos
Experiência da empresa	30 pontos

Critério de Avaliação	Pontuação Máxima
Metodologia de execução	20 pontos
Segurança da informação e capacidade operacional	10 pontos
Plano de execução e qualidade das entregas	5 pontos
Pontuação Técnica Máxima (PT)	100 pontos

8.3. Serão classificadas tecnicamente as propostas que obtiverem, no mínimo, 60 (sessenta) pontos na avaliação técnica.

8.4. A avaliação econômica será realizada mediante atribuição de pontuação proporcional às propostas apresentadas, sendo conferidos 100 (cem) pontos à proposta de menor preço, aplicando-se às demais a seguinte fórmula:

$$PP = (MP \div P) \times 100$$

Onde:

- PP = Pontuação de Preço;
- MP = Menor preço válido apresentado;
- P = Valor da proposta em avaliação.

8.5. A classificação final observará a combinação da pontuação técnica e da pontuação econômica, conforme a seguinte ponderação:

$$\textbf{Pontuação Final} = (\textbf{Pontuação Técnica} \times 70\%) + (\textbf{Pontuação de Preço} \times 30\%)$$

Será considerada vencedora a proponente que obtiver a maior pontuação final.

8.6. A pontuação técnica será atribuída mediante análise objetiva dos seguintes critérios:

8.6.1. Qualificação da equipe técnica (35 pontos):

- qualificação e experiência dos profissionais indicados;
- certificações reconhecidas em segurança ofensiva (OSCP, CEH, GPEN, GXPN ou equivalentes);
- indicação do responsável técnico e comprovação de vínculo com a empresa.

8.6.2. Experiência da empresa (30 pontos):

- experiência comprovada na execução de serviços de Pentest compatíveis com o objeto;
- quantidade de projetos executados nos últimos cinco anos;
- atuação em ambientes críticos, aplicações web, APIs, infraestrutura e ambientes em nuvem.

8.6.3. Metodologia de execução (20 pontos):

- aderência às metodologias OWASP Testing Guide, NIST SP 800-115, PTES ou equivalentes;
- metodologia de execução dos testes;
- processo de validação das vulnerabilidades e realização do reteste.

8.6.4. Segurança da informação e capacidade operacional (10 pontos):

- procedimentos de confidencialidade;
- proteção das informações obtidas durante os testes;
- controles de acesso e gestão das evidências.

8.6.5. Plano de execução e qualidade das entregas (5 pontos):

- planejamento dos trabalhos;
- execução dos testes;
- elaboração dos relatórios de auditoria;
- realização do reteste;
- emissão do relatório de auditoria final contendo as vulnerabilidades remanescentes e as correções validadas.

8.7. O regime de execução do contrato será o de empreitada por preço global, compreendendo a execução integral dos serviços de auditoria especializada em *Pentest* e Reteste, incluindo todas as atividades previstas neste Termo de Referência.

8.8. Para fins de habilitação, a proponente deverá comprovar sua regularidade jurídica, fiscal, trabalhista, econômico-financeira e técnica, mediante apresentação da documentação exigida nos itens subsequentes deste Termo de Referência.

8.9. A licitante deverá declarar cumprimento das normas de saúde e segurança do trabalho; observância das vedações legais aplicáveis à contratação de mão de obra e disponibilidade de equipe, capacidade técnica e recursos necessários para execução integral do objeto.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O valor estimado da contratação é de **R\$ 65.000,00**, correspondente ao limite máximo admitido para a presente contratação, tendo sido definido com base em pesquisa de mercado e em contratações similares de serviços especializados de auditoria com a realização de *pentest* e reteste, em conformidade com o Decreto estadual nº 67.888, de 17 de agosto de 2023.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Fundação Prevcom.

11. DISPOSIÇÕES FINAIS

11.1. A proponente deverá indicar, em sua proposta, endereço eletrônico oficial para comunicações, responsabilizando-se por sua atualização e pelo acompanhamento das mensagens encaminhadas pela CONTRATANTE.

11.2. A contratação será formalizada por meio de Ordem de Fornecimento, instrumento equivalente ou contrato, conforme definido pela CONTRATANTE, podendo os documentos e comunicações serem emitidos e encaminhados por meio eletrônico.

11.3. A proponente é responsável pela veracidade das informações e dos documentos apresentados, sujeitando-se às sanções administrativas e legais cabíveis em caso de falsidade ou irregularidade.

11.4. Os custos relativos à elaboração e apresentação da proposta correrão exclusivamente por conta da proponente, não cabendo qualquer ressarcimento.

11.5. A CONTRATANTE poderá revogar ou anular o procedimento de contratação, no todo ou

em parte, mediante justificativa, nos termos da legislação aplicável.

11.6. Os casos omissos serão resolvidos pela CONTRATANTE, observadas as disposições da Lei nº 14.133/2021 e demais normas aplicáveis.

Despacho: Encaminho o presente Termo de Referência à apreciação da autoridade competente, para análise e aprovação, visando ao prosseguimento da contratação dos serviços descritos neste documento.

Sueli Meschke Mendes Starke Rodrigues

Auditora-chefe

Despacho: Aprovo o presente Termo de Referência e autorizo o prosseguimento do processo de contratação, observadas as disposições da Lei nº 14.133/2021 e demais normas aplicáveis.

SYLVIO EUGENIO

Diretor-Presidente

Autoridade competente



Documento assinado eletronicamente por **Sueli Meschke Mendes Starke Rodrigues, Assessor IV**, em 30/06/2026, às 11:09, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



Documento assinado eletronicamente por **Sylvio Eugenio De Araujo Medeiros, Diretor Presidente**, em 30/06/2026, às 18:07, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



A autenticidade deste documento pode ser conferida no site

[https://sei.sp.gov.br/sei/controlador_externo.php?](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador 0112664817 e o código CRC 27A3FEF8.