COTIAPREV
Instituto de Previdência de Cotia

RESPOSTA À IMPUGNAÇÃO Nº 02

PREGÃO ELETRÔNICO Nº 05/IPSPMC/2026 — PROCESSO ADMINISTRATIVO Nº 0901/2026

Impugnante: SELF ASSESSORIA E CONSULTORIA LTDA, CNPJ nº 10.450.122/0001-33.

Objeto do certame: licença de uso de sistema integrado de gestão previdenciária, com implantação, conversão da base de dados, parametrização, treinamento, suporte técnico continuado e serviços técnicos sob demanda.

Itens impugnados: subitens 2.6.2, alínea "e", e 2.6.2.2 do Termo de Referência (Anexo I do Edital) — critérios para a demonstração de controles de segurança da informação equivalentes à certificação ISO/IEC 27001 do datacenter.

I — ADMISSIBILIDADE

A impugnação foi recebida em 29 de outubro de 2026, pela plataforma BLL Compras, antes do termo final de 06 de novembro de 2026, correspondente ao 3º (terceiro) dia útil anterior à data de abertura do certame, e foi apresentada por pessoa legitimada, nos termos do art. 164 da Lei nº 14.133/2021 e dos subitens 17.1 e 17.2 do Edital. É, portanto, tempestiva e dela se conhece.

II — SÍNTESE DAS ALEGAÇÕES

A impugnante não se opõe à exigência de segurança da informação do datacenter. Sustenta, em síntese, que o subitem 2.6.2, alínea "e", do Termo de Referência admite a demonstração de controles equivalentes à certificação ISO/IEC 27001, documentados e auditáveis, sem definir os requisitos técnicos mínimos que caracterizam a equivalência, os documentos aceitos e a metodologia de avaliação, o que poderia gerar interpretações divergentes e margem excessiva de discricionariedade, e que, sendo a comprovação exigida após a contratação, os critérios devem ser conhecidos desde a fase de disputa.

Requer: (a) o recebimento e a análise da impugnação; (b) a retificação dos subitens 2.6.2, alínea "e", e 2.6.2.2 do Termo de Referência; (c) a definição dos requisitos mínimos, das evidências aceitas e da metodologia de avaliação; (d) o esclarecimento de que os mesmos parâmetros serão aplicados a qualquer fornecedor e a qualquer modalidade de comprovação; (e) a definição do prazo de apresentação da documentação e do procedimento de análise, inclusive quanto à complementação; (f) caso a retificação altere as condições de formulação das propostas, a observância do art. 55, §1º, da Lei nº 14.133/2021; e (g) subsidiariamente, a prestação de esclarecimentos formais e objetivos sobre os critérios de equivalência, com divulgação pelos mesmos meios do instrumento convocatório.

III — ANÁLISE

1. Natureza e alcance da exigência. A exigência do subitem 2.6.2, alínea "e", do Termo de Referência constitui requisito de execução contratual, e não de habilitação (subitem 2.6.2.1). Na habilitação exige-se apenas declaração de compromisso (subitem 10.6, alínea "k", do Edital e Modelo K do Anexo IV), e a comprovação é obrigação da contratada (Cláusula Sétima, alínea "p", da Minuta do Contrato). A exigência recai sobre o datacenter utilizado, e não sobre a licitante, nos termos do subitem 2.6.2.2 do Termo de Referência, que registra: "A norma ISO/IEC 27001 é padrão internacional amplamente difundido entre provedores de infraestrutura".

O modelo observa a Súmula nº 17 do Tribunal de Contas do Estado de São Paulo, segundo a qual "em procedimento licitatório, não é permitido exigir-se, para fins de habilitação, certificações de qualidade ou quaisquer outras não previstas em lei", e o entendimento do Tribunal de Contas da União no Acórdão nº

1.085/2011-Plenário, que considerou inadmissível o emprego da certificação ISO como exigência de habilitação.

2. Fundamento legal. A solução tratará dados pessoais de servidores, aposentados e pensionistas, inclusive dados sensíveis referentes à saúde, constantes dos laudos e registros de perícia médica (subitem 3.15 do Termo de Referência e art. 5º, inciso II, da Lei nº 13.709/2018), além de dados financeiros, como remunerações, proventos, dados bancários e consignações, relativos a titulares em grande parte idosos, categorias que figuram entre os critérios adotados pela Autoridade Nacional de Proteção de Dados para caracterizar o risco ou dano relevante decorrente de incidente de segurança (art. 5º, incisos I, II e III, do Regulamento de Comunicação de Incidente de Segurança, aprovado pela Resolução CD/ANPD nº 15/2024).

O COTIAPREV figura como controlador e a contratada como operadora (subitem 11.1 do Termo de Referência e subitem 16.1 do Edital). A Lei nº 13.709/2018 impõe aos agentes de tratamento a adoção de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais, desde a fase de concepção do produto ou do serviço até a sua execução (art. 46, caput e §2º), obriga todo aquele que intervém no tratamento a garantir a segurança da informação (art. 47), exige que os sistemas sejam estruturados de forma a atender aos requisitos de segurança e aos padrões de boas práticas e de governança (art. 49) e determina que o operador realize o tratamento segundo as instruções do controlador, que verificará a observância dessas instruções e das normas sobre a matéria (art. 39). O operador que descumprir a legislação de proteção de dados ou as instruções lícitas do controlador responde solidariamente pelos danos causados (art. 42, §1º, inciso I).

O padrão de segurança é, portanto, definido pela Administração, na condição de controladora, a partir da lei e do interesse público, e não se ajusta à infraestrutura que determinado fornecedor pretenda utilizar.

3. Requisitos mínimos. A Lei nº 13.709/2018 não enumera controles técnicos de segurança, atribuindo à autoridade nacional a possibilidade de dispor sobre padrões técnicos mínimos (art. 46, §1º). Na ausência de enumeração legal, o Termo de Referência adotou como parâmetro objetivo a norma ISO/IEC 27001, padrão internacional público e de conhecimento corrente entre os provedores de infraestrutura. Assim, os requisitos mínimos são os da própria norma: os "controles equivalentes" a que se refere o subitem 2.6.2, alínea "e", são os controles de segurança da informação do Anexo A da ISO/IEC 27001, selecionados e justificados segundo a metodologia da própria norma, que exige a elaboração de Declaração de Aplicabilidade com a indicação dos controles necessários, da justificativa de sua inclusão, de sua implementação e da justificativa para a exclusão de qualquer controle do Anexo A (item 6.1.3, alínea "d", da ISO/IEC 27001).

A Administração não criou rol próprio de controles nem admitiu subconjunto reduzido da norma, o que rebaixaria o nível de proteção dos dados e quebraria a isonomia em relação aos licitantes que utilizarem provedor certificado. A equivalência exige que os controles adotados correspondam, em extensão e conteúdo, aos que seriam exigidos para a certificação, cabendo à licitante que optar pela alternativa conhecer a norma e demonstrar o seu atendimento.

4. Ônus da comprovação. Mantida a exigência de certificação ISO/IEC 27001, o ônus de demonstrar a segurança do datacenter é integralmente da contratada. Na hipótese de controles equivalentes, a contratada deverá demonstrá-los de forma documentada e auditável, isto é, passível de ser auditada, nos termos do subitem 2.6.2, alínea "e", do Termo de Referência.

A exigência atende, ainda, ao princípio da responsabilização e prestação de contas, que impõe ao agente de tratamento a demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia dessas medidas (art. 6º, inciso X, da Lei nº 13.709/2018).

A conformidade com a ISO/IEC 27001 interessa, assim, à própria contratada: é o meio pelo qual poderá demonstrar, diante de eventual incidente, que não houve violação à legislação de proteção de dados (art. 43, inciso II, da Lei nº 13.709/2018), e é considerada na gradação de eventuais sanções da autoridade nacional, que leva em conta a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano e a adoção de política de boas práticas e governança (art. 52, §1º, incisos VIII e IX, da mesma Lei).

5. Ausência de alteração das condições de formulação das propostas. A presente resposta apenas reafirma o conteúdo da obrigação já prevista no subitem 2.6.2, alínea "e", do Termo de Referência, à qual todos os licitantes se comprometem desde a habilitação, e não cria obrigação nova. O licitante que utilizar datacenter certificado — prática amplamente difundida entre os provedores de infraestrutura, como registra o subitem 2.6.2.2 — comprovará a exigência apenas com o certificado. Não há, assim, alteração do Edital e, por conseguinte, alteração que comprometa a formulação das propostas, razão pela qual não incidem o art. 55, §1º, da Lei nº 14.133/2021 e o subitem 17.5 do Edital, mantida a data da sessão pública.

IV — CONCLUSÃO

Diante do exposto, esta Agente de Contratações manifesta-se pelo CONHECIMENTO da impugnação e, no mérito, pela sua IMPROCEDÊNCIA, por inexistir irregularidade nos subitens 2.6.2, alínea "e", e 2.6.2.2 do Termo de Referência, cujo parâmetro de equivalência é a própria norma ISO/IEC 27001, restando prejudicado o pedido "f", uma vez que não há alteração do Edital. Mantêm-se inalterados o Edital, seus Anexos e a data de abertura da sessão pública, em 11 de novembro de 2026, às 09h00min. Submetem-se os autos à autoridade competente para decisão, na forma do art. 25, inciso III, do Decreto Municipal de Cotia nº 9.261/2023.

Cotia/SP, 03 de novembro de 2026.

RUTE DA SILVA SOUZA AMARAL
Agente de Contratações/Pregoeira
Portaria COTIAPREV nº 149/2026, de 15 de outubro de 2026

DECISÃO

Acolho a manifestação da Agente de Contratações, pelos seus próprios fundamentos, e DECIDO pelo CONHECIMENTO da Impugnação nº 02, apresentada por SELF ASSESSORIA E CONSULTORIA LTDA, e, no mérito, pela sua IMPROCEDÊNCIA, mantidos o Edital, seus Anexos e a data da sessão pública. Dê-se ciência à impugnante e publique-se na plataforma BLL Compras, no Portal Nacional de Contratações Públicas — PNCP e no sítio eletrônico oficial do COTIAPREV, na forma do art. 164, parágrafo único, da Lei nº 14.133/2021.

Cotia/SP, 03 de novembro de 2026.

RODRIGO KAWAMURA
Diretor-Presidente

IMPUGNAÇÃO AO EDITAL DO PREGÃO ELETRÔNICO Nº 05/IPSPMC/2026

PROCESSO ADMINISTRATIVO Nº 0901/2026
AO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE COTIA - COTIAPREV

Assunto: Questionamento da ausência de critérios objetivos para comprovação de controles de segurança da informação equivalentes à ISO/IEC 27001.

SELF ASSESSORIA E CONSULTORIA LTDA, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 10.450.122/0001-33, vem, respeitosamente, apresentar **IMPUGNAÇÃO AO EDITAL DO PREGÃO ELETRÔNICO Nº 05/IPSPMC/2026**, referente ao Processo Administrativo nº 0901/2026, com fundamento no art. 164 da Lei nº 14.133/2021, pelos motivos a seguir expostos.

I - DO OBJETO DO QUESTIONAMENTO

O certame tem por objeto a contratação de empresa especializada para o fornecimento de licença de uso de sistema integrado de gestão previdenciária para Regime Próprio de Previdência Social - RPPS, abrangendo módulos de folha de pagamento, recursos humanos, concessão de benefícios, COMPREV e demais funcionalidades, além dos serviços de implantação, conversão de dados, treinamento e suporte técnico.

O item 2.6.2, alínea "e", do Termo de Referência estabelece que a contratada deverá comprovar que o datacenter utilizado possui certificação ISO/IEC 27001 ou, alternativamente, demonstrar a adoção de controles equivalentes de segurança da informação, documentados e auditáveis.

Por sua vez, o subitem 2.6.2.2 esclarece que a alternativa foi prevista para não excluir fornecedores cujo datacenter, embora seguro, não detenha a certificação formal.

Entretanto, embora o instrumento convocatório admita expressamente a comprovação por meios alternativos, não estabelece quais requisitos técnicos mínimos caracterizam a equivalência, quais documentos poderão ser apresentados ou quais parâmetros serão utilizados pela Administração para avaliar a suficiência dos controles adotados.

A presente impugnação não pretende afastar a necessidade de segurança da informação na contratação, mas assegurar que a alternativa expressamente admitida

pelo próprio edital seja regulamentada por critérios claros, objetivos e previamente conhecidos por todos os interessados.

II – DA AUSÊNCIA DE CRITÉRIOS OBJETIVOS PARA A AVALIAÇÃO DA EQUIVALÊNCIA

A certificação ISO/IEC 27001 está relacionada à gestão da segurança da informação. Sua exigência pode ser pertinente à contratação de uma solução previdenciária que envolve dados funcionais, financeiros e previdenciários, além de informações pessoais dos servidores, aposentados e pensionistas.

Todavia, o próprio Termo de Referência reconhece que a certificação formal não é a única maneira de demonstrar a adoção de medidas adequadas de segurança.

O problema está na ausência de definição objetiva sobre o que será considerado equivalente à certificação. Não foram identificados, nos dispositivos examinados, parâmetros que permitam aos licitantes conhecer antecipadamente os controles mínimos exigidos, as evidências documentais aceitas e a metodologia de avaliação que será aplicada pela Administração.

Essa omissão pode gerar interpretações divergentes quanto ao atendimento da obrigação contratual, deixando os fornecedores sem condições de avaliar previamente se a infraestrutura que utilizam será considerada adequada.

Também pode conferir excessiva margem de discricionariedade à análise posterior, com risco de decisões inconsistentes entre fornecedores que apresentem medidas de segurança de natureza semelhante.

A previsão de controles equivalentes somente cumpre sua finalidade de ampliar as possibilidades de atendimento se houver critérios que permitam verificar, de maneira objetiva e isonômica, a efetiva proteção das informações.

Dessa forma, solicita-se a complementação do instrumento convocatório, com a definição dos requisitos técnicos mínimos e dos meios de comprovação admitidos para a demonstração de equivalência à ISO/IEC 27001.

III – DA COMPROVAÇÃO POSTERIOR À CONTRATAÇÃO

O edital prevê que a comprovação documental referente à certificação do datacenter ou aos controles equivalentes será exigida após a contratação.

O adiamento da apresentação documental, por si só, não constitui o objeto principal desta impugnação. Entretanto, torna ainda mais importante que os critérios de avaliação estejam definidos previamente, pois o contratado deverá conhecer, desde a fase de disputa, as condições que precisará demonstrar para cumprir a obrigação.

A ausência de parâmetros objetivos pode gerar incerteza quanto à documentação necessária, à suficiência dos controles adotados e às condições para aceitação da infraestrutura escolhida.

Por essa razão, solicita-se que a Administração esclareça expressamente quais requisitos deverão ser atendidos, quais evidências serão aceitas e como ocorrerá a análise da documentação apresentada após a contratação.

Deve-se esclarecer, ainda, se serão aceitos relatórios de auditoria independente, políticas e procedimentos documentados de segurança, evidências de controles de acesso, mecanismos de backup e recuperação, gestão de incidentes e outros elementos técnicos pertinentes, desde que demonstrem, de forma verificável, o atendimento aos requisitos definidos pela Administração.

A indicação desses exemplos não pretende substituir a avaliação técnica do órgão, mas evidenciar a necessidade de estabelecer previamente quais elementos serão considerados suficientes para a comprovação da equivalência.

IV – DOS PEDIDOS

Diante do exposto, requer-se:

a) O recebimento e a análise da presente manifestação, com apreciação dos fundamentos apresentados, observadas as disposições legais e regulamentares aplicáveis.

b) A retificação do Termo de Referência, especialmente dos subitens 2.6.2, alínea "e", e 2.6.2.2, para estabelecer critérios técnicos objetivos para a aceitação de controles de segurança da informação equivalentes à certificação ISO/IEC 27001.

c) A definição dos requisitos mínimos de segurança, dos documentos e das evidências técnicas aceitos para comprovar a equivalência, bem como da metodologia que será utilizada pela Administração para avaliar sua suficiência.

d) O esclarecimento de que a documentação e os controles apresentados serão avaliados segundo os mesmos parâmetros técnicos, independentemente do fornecedor do datacenter ou da modalidade de comprovação adotada.

e) A definição do prazo para apresentação da documentação após a contratação e do procedimento de análise, incluindo os critérios de aceitação e as providências cabíveis em caso de necessidade de complementação documental.

f) Caso a retificação implique alteração das condições relevantes para a formulação das propostas, a adoção das providências previstas no art. 55, § 1º, da Lei nº 14.133/2021, inclusive a divulgação da alteração e a reabertura dos prazos cabíveis, conforme o caso.

g) Subsidiariamente, caso não se entenda necessária a alteração do edital, que sejam prestados esclarecimentos formais e objetivos sobre os critérios de equivalência, com divulgação pelos mesmos meios utilizados para dar publicidade ao instrumento convocatório.

Termos em que, pede deferimento.

Paraíso do Tocantins, 29 de outubro de 2026.

SELF ASSESSORIA E CONSULTORIA LTDA:10450122000133

Assinado de forma digital por SELF ASSESSORIA E CONSULTORIA LTDA:10450122000133
Dados: 2026.10.29 14:25:38 -03'00'

SELF ASSESSORIA E CONSULTORIA LTDA
IRINEU PEREIRA DE SOUZA
Sócio Diretor