

---

## RESPOSTA AO PEDIDO DE IMPUGNAÇÃO 01/2024

---

Belo Horizonte, 02 de agosto de 2024

Trata-se de Impugnação ao Edital do Pregão Eletrônico Sesc em Minas n.º 000111/2024 – Processo nº 004001-06640, cujo objeto é contratação de empresa especializada na prestação de serviços para fornecimento e implantação de software de atendimento para a operação da Central de Relacionamento do Sesc em Minas, contemplando uma solução omnichannel, abarcando funcionalidades de gestão, monitoramento e atendimento ativo e receptivo por meio de diversos canais, como telefone, webchat, e-mail, WhatsApp e redes sociais (Instagram e Facebook), incluindo implantação, instalação, configuração, integração, ambiente de testes, treinamento de uso, operação assistida, suporte técnico, customização e parametrização. A solução contemplará interações humanas e digitais (eletrônica e bot), sendo possível a utilização dos recursos por meio de um assistente virtual. O modelo SaaS será adotado para o fornecimento do software, englobando todos os recursos indispensáveis e necessários para a execução e prestação dos serviços (exceto espaço físico e mão de obra operacional).

### 1 - DA TEMPESTIVIDADE

Conforme item 4.1. do Edital convocatório, o prazo fatal para a apresentação de impugnação é de até 03 (três) dias úteis anteriores à data de abertura da Sessão de Licitação, excluindo-se da contagem a data da sessão, programada para 06/08/2024. Dessa forma, considerando que a impugnação foi apresentada em 29/07/2024, esta foi tempestiva.

### 2 – DA IMPUGNAÇÃO

Desta feita, abaixo transcrevemos trechos para entendimento do ponto impugnado, em síntese, é impugnado a exigência das certificações ISO 27001 e SOC 2, alegando a impugnante o seguinte:

“(…) 1. DO POSSÍVEL DIRECIONAMENTO DO CERTAME E DA AFRONTA À COMPETITIVIDADE

Os pontos do edital que estão sendo impugnados aqui se referem aos itens que exigem a apresentação das certificações ISO 27001 e SOC2 como condicionantes à aceitabilidade das propostas. O motivo que fundamenta a necessidade de exclusão ou reforma desses itens é que, a disposição neles existente, se mantida, afronta a competitividade do certame, uma vez que, antes mesmo da classificação das propostas poderia beneficiar um licitante específico que possua tais certificações, em detrimento de outros licitantes, que tenham apresentado propostas mais vantajosas e que atendam aos

requisitos técnicos da norma, mas que por qualquer motivo não tenham se submetido ao processo de acreditação para ostentar a certificação em tela.

#### 1.1. DA AFRONTA À COMPETITIVIDADE (Exigência de Certificação Específica)

Inicialmente, o disposto nos itens impugnados viola os termos DO REGULAMENTO DE LICITAÇÕES E CONTRATOS DO SESC E DO SENAC e a jurisprudência consolidada do Tribunal de Contas da União. Para que fique claro, destacamos o texto dos itens que serão impugnados:

7.16.3.1. Juntamente com a proposta adequada os licitantes deverão encaminhar:

7.16.3.1.1. Anexo II - Requisitos Técnicos Obrigatórios da Solução Tecnológica e Anexo III - Requisitos Funcionais Obrigatórios, devidamente preenchidos;

7.16.3.1.2. Certificações ISO 27001 e SOC-2, sendo necessário que estas certificações sejam específicas da própria solução ofertada, não sendo aceitos certificados do Data Center ou da nuvem.

Em que pese a previsão constante no art. 26, §5º do novel Regulamento de Licitações e Contratos do SESC e do SENAC<sup>1</sup>, entende-se que a referida exigência é completamente abusiva, tendo fortes indícios de uma possível destinação a um licitante específico, uma vez que, os itens impugnados estabeleceram expressamente a exigência de que a licitante vencedora, antes da contratação e como critério de classificação da proposta, comprove que possui certificados específicos ativos, quais sejam as certificações ISO 27001 e SOC-2 (vide item 7.16.3.1.2), sem que tais certificações se demonstrem imprescindíveis para atestar a aderência aos requisitos exigidos para

1 § 5.º Poderão ser exigidos, como critério de classificação de proposta, certificado, laudo ou documento análogo que tenha capacidade de demonstrar a qualidade do objeto ou processo de fabricação, emitido por instituição oficial competente ou por instituição credenciada, e/ou comprovação de que o objeto atende às normas técnicas determinadas pelos órgãos oficiais competentes. (Incluído pelas Resoluções Sesc n.º 1.593/2024 e Senac n.º 1.270/2024) obtenção desses certificados, eis que, qualquer licitante pode atender às exigências de qualificação técnica ainda que não tenha obtido, por qualquer razão, as referidas certificações.

Deve ser ressaltado que, o SESC não está impedido de, após a contratação, exigir e conceder prazo para que a licitante contratada obtenha a certificação desejada. Contudo, na fase de concorrência e contratação, não se mostra razoável exigir, sob pena de desclassificação, prova de certificação específica das licitantes. O que se revela importante, no momento da contratação, É VERIFICAR SE HÁ A CAPACIDADE TÉCNICA PARA REALIZAÇÃO DOS SERVIÇOS PARA SATISFAÇÃO DO OBJETO A SER CONTRATADO.

Nesse mesmo sentido tem sido o entendimento atual do Tribunal de Contas da União. A título de exemplo, temos o voto do Ilustríssimo Ministro, Ubiratan Aguiar, então relator do Processo TC nº 001.142/2002-7, constante no Acórdão TCU 1526/2002-Plenário, tratou-se da exigência da certificação ISO 9001, concluindo-se que:

“(…)

Voto:

Verifico que dos três pontos questionados na presente representação, cujas justificativas foram aceitas pela Unidade Técnica, dois merecem maior análise por este Tribunal, os quais passarei a comentar.

2. O primeiro item diz respeito à exigência da Certificação ISO 9001 para fins de habilitação. Este Tribunal, como bem colocado pela instrução precedente, já se manifestou no sentido de que essa exigência não poderia ser feita para fins de inabilitação. Ou seja, O PESO DADO A ESSA CERTIFICAÇÃO NÃO PODE ULTRAPASSAR SUA IMPORTÂNCIA REAL.

3. NESSE SENTIDO, TRAGO À COLAÇÃO ENSINAMENTO DE MARÇAL JUSTEN FILHO, QUE AO COMENTAR ACERCA DA CERTIFICAÇÃO ISO 9000, assim se pronunciou:

" ...Uma empresa pode preencher todos os requisitos para obtenção da certificação, mas nunca ter tido interesse em formalizar esse resultado. Exigir peremptoriamente a certificação como requisito de habilitação equivaleria a tornar compulsória uma alternativa meramente facultativa: nenhuma lei condiciona o exercício de alguma atividade à obtenção do Certificado ISO 9000. Portanto, obtém a certificação quem o desejar (e preencher os requisitos, é óbvio).

Em outras palavras, O ESSENCIAL NÃO É A CERTIFICAÇÃO FORMAL, MAS O PREENCHIMENTO DOS REQUISITOS NECESSÁRIOS À SATISFAÇÃO DO INTERESSE PÚBLICO. SE O SUJEITO PREENCHE OS REQUISITOS, MAS NÃO DISPÕE DA CERTIFICAÇÃO, NÃO PODE SER

IMPEDIDO DE PARTICIPAR DO CERTAME." ("Comentários à Lei de Licitações e Contratos Administrativos", 8º Edição, Editora Dialética, 2001, fl. 349)

(...)"

No mesmo sentido andou o Colendo TCU, conforme restou consignado no Acórdão 854/2013 - TCU - Plenário, onde se tratava das certificações CMMI e MPS.BR (análogas), senão vejamos:

"Voto

(...)

É pacífica a jurisprudência deste Tribunal no sentido de que, nos termos do Entendimento III, da Nota Técnica SEFTI/TCU 5/2010, 'é vedada a exigência de certificado de qualidade de processo de software - a exemplo de CMMI ou MPS.BR - como requisito para habilitação em licitação, por ausência de previsão legal, por implicar em despesas anteriores à contratação e desnecessárias à competição e por ferir a isonomia, restringindo injustificadamente a competição', como se depreende dos Acórdãos nºs 2.521/2008, 1.287/2008, 2.533/2008, e 189/2009, todos do Plenário, e 5.736/2011-1ºC.

(...)

6.1.2 Todavia, nos termos do Entendimento V, da Nota Técnica SEFTI/TCU 5/2010, é 'possível incluir, na especificação técnica dos serviços a serem realizados, todos os resultados esperados que, segundo modelos de qualidade de processo aderentes à norma ABNT NBR ISO/IEC 15.504, tais como CMMI ou MPS.BR, caracterizam um dado nível de capacidade de processo de software, desde que tal nível reflita as escolhas estratégicas da organização para o seu processo de software e a sua real capacidade de avaliar tecnicamente os artefatos e produtos entregues' (Acórdão nº 5.736/2011-1ªC).

6.1.3 É também aceita a exigência de certificações de qualidade COMO CRITÉRIO DE PONTUAÇÃO TÉCNICA ADICIONAL, como foi aludido nos Acórdãos 479/2004, 1094/2004, 2048/2006, 539/2007 e 891/2008, todos do Plenário, porém, ainda sim, como assentado no Acórdão nº 10/2008-P, DESDE QUE TAIS CRITÉRIOS GUARDEM CORRELAÇÃO DIRETA COM A QUALIDADE DOS SERVIÇOS A SEREM PRESTADOS.

(...)"

Vê-se, portanto, a partir da leitura da jurisprudência indicada, que O ESSENCIAL NÃO É A CERTIFICAÇÃO FORMAL, MAS O PREENCHIMENTO DOS REQUISITOS NECESSÁRIOS À SATISFAÇÃO DO OBJETO A SER CONTRATADO. Daí o entendimento de que é possível incluir os requisitos que devam ser atendidos pelo produto ou serviço, inclusive os exigidos para a certificação, diretamente no termo de referência e/ou edital, em vez de se exigir qualquer certificação, por menos específica que seja.

#### 1.1.1 SOBRE AS CERTIFICAÇÕES

##### ISO 27001

A ISO 27001 é uma norma internacional que especifica os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). A certificação dessa norma é altamente valorizada e muitas vezes requisitada para assegurar que as organizações tenham controles adequados para proteger a informação sensível. No contexto de soluções em nuvem, é fundamental entender a responsabilidade compartilhada entre o provedor de nuvem (como AWS, Azure ou Google Cloud) e o prestador de serviços que utiliza essa infraestrutura para oferecer suas soluções.

##### SOC 2

Já a certificação SOC 2 é um padrão que avalia os controles de segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade de uma organização. Ela é frequentemente solicitada para garantir que um prestador de serviços em nuvem possui controles adequados para proteger dados sensíveis. No entanto, assim como citado sobre a ISO 27001, no ambiente de computação em nuvem, é importante compreender a distinção de responsabilidades entre o provedor de nuvem (por exemplo, AWS, Azure ou Google Cloud) e o prestador de serviços que utiliza essa infraestrutura.

##### Modelo de Responsabilidade Compartilhada

É importante compreender que em ambientes de nuvem, a segurança e a conformidade são compartilhadas entre o provedor de nuvem e o prestador de serviços. Este modelo de responsabilidade compartilhada delineia claramente as responsabilidades de cada parte:

- Provedor de Nuvem: Responsável pela segurança da infraestrutura subjacente, incluindo datacenters, hardware, redes e hipervisores.

- Prestador de Serviços: Responsável pela segurança das aplicações, configuração dos serviços em nuvem e gerenciamento dos dados dentro do ambiente de nuvem.

#### Escopo da Certificação ISO 27001

A certificação ISO 27001 se aplica ao escopo específico do SGSI da organização. Quando se trata de um provedor de serviços que utiliza uma solução em nuvem, o escopo do SGSI da certificação do prestador de serviços deve focar nas áreas que estão sob seu controle direto, como as configurações da aplicação, políticas de acesso e tratamento dos dados.

Para os provedores de nuvem, a certificação ISO 27001 abrange a segurança da infraestrutura e dos serviços que fornecem. Esses provedores, como parte de seus compromissos de segurança, já possuem certificações de conformidade que demonstram que seguem as melhores práticas internacionais para garantir a segurança da sua infraestrutura.

#### Escopo da Certificação SOC 2

A certificação SOC 2 é baseada nos critérios de confiança (Trust Services Criteria) que avaliam a eficácia dos controles relacionados à segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade. O escopo da certificação SOC 2 deve ser aplicado onde os controles e processos estão sob o controle direto da organização.

É sabido que os principais provedores de nuvem já possuem certificações SOC 2 que validam a eficácia de seus controles de segurança e operação da infraestrutura. Isso inclui a segurança física dos datacenters, a segurança de rede, a manutenção do hardware e os controles de acesso aos sistemas subjacentes.

#### Redundância e Eficiência de Recursos

Exigir que um prestador de serviços obtenha a certificação ISO 27001 e/ou SOC 2 para áreas que são controladas pelo provedor de nuvem seria redundante e desnecessário. Isso pode levar a um aumento desproporcional dos custos e esforços sem proporcionar benefícios adicionais significativos, uma vez que essas áreas já são cobertas pela certificação do provedor de nuvem.

#### Foco nos Controles Relevantes

Os prestadores de serviços em nuvem devem focar em obter certificações e manter controles que estão diretamente sob sua gestão, como a segurança

das suas aplicações, gestão de acessos, proteção de dados e configuração segura dos serviços em nuvem. As certificações SOC 2 e/ou ISO 27001 do provedor de nuvem já assegura que os componentes de infraestrutura subjacentes atendem aos critérios de confiança necessários.

Com efeito, ao considerar as certificações ISO 27001 e SOC 2, é essencial focar no escopo de controle e responsabilidade. A certificação deve ser exigida do provedor de nuvem para garantir que a infraestrutura e os serviços de base são seguros e conformes. O prestador de serviços deve, por sua vez, garantir que suas práticas de segurança e conformidade para as aplicações e dados gerenciados na nuvem estão em conformidade com os critérios de confiança relevantes, sem a necessidade de duplicação de certificação para a infraestrutura já coberta pelo provedor de nuvem. Isso promove uma abordagem eficiente e eficaz para a segurança e conformidade em soluções baseadas na nuvem.

Ao mesmo tempo, caso esse respeitável Serviço Social do Comércio decida por retirar o item impugnado e inserir no edital ou no TR os requisitos exigidos para a certificação, ainda assim, será necessário adotar tal medida de forma que não sejam exigidas características tão específicas que só pudessem ser atendidas por aqueles que tivessem se submetido àquela determinada certificação, principalmente quando INEXISTE PARECER TÉCNICO, ELABORADO POR PESSOAL ESPECIALIZADO, QUE EXPLICITE DETALHADA E JUSTIFICADAMENTE QUAIS NECESSIDADES RELEVANTES PARA O SESC DEIXARIAM DE SER ATENDIDAS NO CASO DE ADOÇÃO DE OUTRAS NORMAS SEMELHANTES COMO ALTERNATIVA.

Por todos esses motivos, pugna-se pela anulação do item 7.16.3.1. e de seus subitens 7.16.3.1.1 e 7.16.3.1.2, do Termo de Referência, ante a sua evidente ilegalidade, expurgando-os do ato convocatório impugnado para que o certame seja conduzido sem a existência de disposições ilícitas e sem violação da concorrência/competitividade, respeitando-se assim, os princípios básicos da administração pública.

Ademais, como iremos demonstrar no tópico seguinte, a inclusão dessas exigências em item diverso ao da descrição das capacidades técnicas também demonstram outra forma de irregularidade, podendo ser caracterizada como uma armadilha para as licitantes.

Não bastasse tudo o que foi dito até aqui, é imperioso ressaltar que os itens ora impugnados foram claramente redigidos com o intuito de suavizar uma



exigência eminentemente técnica, demandada de forma precoce - inclusive, como condição de classificação da proposta do licitante - uma vez que se exige não apenas a comprovação de qualificação-técnica usual, já esperada em fase de habilitação ou qualquer momento antes da assinatura do contrato, mas também vincula a própria aceitabilidade da proposta mais vantajosa à comprovação da aderência à normas técnicas específicas, incluindo até mesmo uma norma (SOC2) que sequer conta com a acreditação nacional pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO).

Observe-se que nos itens 4.8 e 8 do ato convocatório impugnado, referente às especificações e fase de julgamento da proposta, ou seja, logo após a etapa de lances e a negociação com o licitante provisoriamente classificado em primeiro lugar, o julgamento das propostas vincula a classificação delas à obediência às especificações técnicas contidas no termo de referência, como se observa abaixo:

4.8. Serão desclassificadas, as propostas que não tiverem 100% de aderência nativo ao ANEXO II – REQUISITOS TÉCNICOS OBRIGATÓRIOS.

(...)

#### 8. DA FASE DE JULGAMENTO

8.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame.

8.2. Será desclassificada a proposta que:

8.2.1. Contiver vícios insanáveis;

8.2.2. NÃO OBEDECER ÀS ESPECIFICAÇÕES TÉCNICAS CONTIDAS NO TERMO DE REFERÊNCIA;

Não bastasse ser exigência eivada de ilicitude como já foi demonstrado por todos os fundamentos e jurisprudência apresentados até aqui, a exigência dos certificados especificados nos itens impugnados, junto com a proposta e como condição de aceitabilidade daquela, é reforçada no ANEXO II do T.R, nos seguintes termos:

A solução deve possuir certificações ISO 27001 e SOC-2, sendo necessário que estas certificações sejam específicas da própria solução ofertada, não sendo aceitos certificados do Data Center ou da nuvem. Os certificados devem ser entregues junto com a proposta.



Ocorre, todavia, que as condições técnicas previstas naquelas normas poderiam muito bem ter sido inseridas nos itens específicos que tratam da capacidade técnica/habilitação técnica detalhados nos anexos ANEXO II - REQUISITOS TÉCNICOS OBRIGATÓRIOS e ANEXO III - REQUISITOS FUNCIONAIS OBRIGATÓRIOS, eis que todos exigem uma série de requisitos de capacidade que PODEM SER COMPROVADOS, INCLUSIVE, MEDIANTE APRESENTAÇÃO DOS ATESTADOS DE CAPACIDADE TÉCNICA-OPERACIONAL, NÃO SENDO NECESSÁRIO PARA TANTO POSSUIR QUALQUER CERTIFICADO EM ESPECÍFICO.

Dito isto, é de se esperar que sejam removidas as exigências contidas nos itens ora vergastados e demais correlatos, ou, caso sejam mantidas, QUE SEJA MANTIDA APENAS A EXIGÊNCIA DE QUE AS LICITANTES ESTEJAM ADERENTES ÀS NORMAS ALMEJADAS, NÃO A EXIGÊNCIA DE APRESENTAÇÃO DE CERTIFICAÇÃO COMO CONDICIONANTE À ACEITABILIDADE DAS PROPOSTAS, e que, em último caso, seja concedido prazo razoável para que, já no curso da execução contratual, a contratada possa vir a obter tais certificações.

Acredita-se, com isso, que o SESC – Minas priorizará a busca pela proposta mais vantajosa, além de prestigiar a isonomia e a competitividade entre as empresas interessadas em participar do processo licitatório em epígrafe.”

### **3 – DA ANÁLISE**

Conforme mencionado anteriormente, a impugnante solicita a retificação do edital para remover a exigência das certificações ISO 27001 e SOC 2.

Pois bem, cabe ressaltar, que segundo as premissas do Regulamento de Licitações e Contratos do Sesc, têm-se que as licitações no âmbito da instituição têm como objetivo a seleção da proposta mais vantajosa e a garantir a legitimidade, a eficiência e a objetividade da aplicação dos recursos do Sesc, bem como o alcance de suas finalidades institucionais.

Assim, cumprirá ao edital traçar em seu corpo, dentre outras diretrizes, aquelas imprescindíveis à aferição da habilitação dos licitantes, de forma que, uma vez preenchidos, presumir-se-á a aptidão do licitante para executar o contrato. Somente desta forma será garantido um julgamento objetivo e isonômico, sem deixar margens a avaliações subjetivas.

Sobre a alegação de possível direcionamento do certame, destacamos que a exigência das certificações ISO 27001 e SOC 2 está em total conformidade com o regulamento de licitações do Sesc, conforme estabelecido na RESOLUÇÃO SESC N.º 1.593/2024. Vejam:

Art. 26, §5.º: Podem ser exigidos certificados, laudos ou documentos análogos que demonstrem a qualidade do objeto ou processo de fabricação emitidos por instituição oficial competente ou por instituição credenciada.

As exigências de certificações ISO 27001 e SOC 2 são justificadas e proporcionais, garantindo que a empresa contratada possua os controles necessários para a segurança e proteção dos dados sensíveis. Essas certificações não configuram direcionamento do certame, mas sim um critério objetivo para assegurar a qualidade e a segurança dos serviços contratados, conforme estabelecido na Resolução SESC N.º 1.593/2024.

Ainda, considerando o caráter técnico da impugnação apresentada, foi encaminhada para área técnica competente, que emitiu o seguinte parecer:

(...) Ao solicitar a certificação da solução contratada o Sesc em Minas se resguarda da prestação dos serviços diretamente contratados e não apenas de uma solução subcontratada pelas preponentes. Essas certificações são internacionalmente reconhecidas e oferecem uma série de benefícios críticos que justificam sua exigência:

**ISO 27001:** A ISO 27001 é uma norma internacional que especifica os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). A certificação ISO 27001 é uma prova de que a empresa possui um sistema de gestão estruturado e eficaz para a proteção de informações sensíveis. Ela abrange vários aspectos da segurança da informação, incluindo:

- **Avaliação de Riscos e Tratamento:** Implementação de uma metodologia de avaliação e tratamento de riscos (como a ISO 31000), que permite identificar, analisar e tratar riscos de segurança da informação de forma sistemática e contínua.
- **Controles de Segurança:** Implementação de uma ampla gama de controles de segurança baseados no Anexo A da ISO 27001, que cobre 114 controles divididos em 14 categorias, incluindo controle de acesso, criptografia, segurança física e ambiental, segurança das operações, segurança das comunicações, aquisição, desenvolvimento e manutenção de sistemas.
- **Gestão de Incidentes de Segurança:** Desenvolvimento e implementação de um processo robusto de gestão de incidentes incluindo a

detecção, resposta e recuperação de incidentes de segurança da informação, minimizando o impacto de possíveis brechas de segurança.

**SOC 2:** A certificação SOC 2 é uma norma desenvolvida pelo American Institute of CPAs (AICPA) que especifica critérios rigorosos para a gestão de dados, baseada nos princípios de confiança: segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade. Apesar de ainda não ser acreditada pelo INMETRO, a SOC 2 é altamente valorizada por diversas razões que justificam sua exigência:

- **Transparência e Confiança:** A certificação SOC 2 exige a implementação de controles de auditoria contínua, como o uso de ferramentas de monitoramento e alertas em tempo real (por exemplo, SIEM - Security Information and Event Management), que garantem a transparência e confiança nas operações de gestão de dados.
- **Segurança e Privacidade dos Dados:** A SOC 2 requer a implementação de controles rigorosos de segurança e privacidade, incluindo criptografia de dados em repouso e em trânsito, gestão de chaves de criptografia, e políticas de acesso baseadas em funções (RBAC - Role-Based Access Control).
- **Mitigação de Riscos:** Empresas certificadas em SOC 2 demonstram ter processos de gestão de riscos robustos, incluindo a realização de avaliações de risco periódicas e a implementação de planos de mitigação de riscos específicos para proteger dados sensíveis.
- **Conformidade com Normas e Regulamentos:** A SOC 2 ajuda as empresas a estarem em conformidade com várias regulamentações de proteção de dados, como a GDPR (General Data Protection Regulation) na Europa e a LGPD (Lei Geral de Proteção de Dados) no Brasil, evitando penalidades e mantendo a integridade organizacional.

Cumpre também ressaltar que o processo licitatório busca selecionar fornecedor em caráter personalíssimo, ou seja, as regras editalícias são estruturadas a partir de requisitos técnicos, econômicos e jurídicos que se amoldam exatamente na necessidade da Instituição licitante. Tanto é verdade que a regra dos contratos oriundos de licitações é proibir a subcontratação total do seu objeto e no máximo permitir a subcontratação parcial e pontual. Nesse sentido, o Sesc em Minas somente pode definir em edital quais condições técnicas a sua contratada deve cumprir, não cabendo exigir condições/certificações de suas terceirizadas e/ou parceiras. Sendo assim, eventuais certificações apresentadas pelas provedoras de espaço em nuvem (AWS, GOOGLE CLOUD) são bem-vindas e mostram diligência em segurança da informação dos potenciais fornecedores, porém, não podem ser exigidas pelo Sesc em Minas no seu edital de licitação. À Instituição licitante, como dito, compete somente exigir condições técnicas dos seus futuros contratados.

Esse raciocínio também se aplica quando avaliada a Lei Geral de Proteção de Dados – LGPD. A Lei define como “agentes de tratamento” duas posições: Controlador e Operador. Define também que compete ao Controlador eleger seus operadores, mas ressalva que esta escolha também carrega responsabilidades: Eventual incidente motivado por falha de um operador

imputa ao Controlador responsabilidade solidária por repará-lo. Senão vejamos:

*Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.*

*§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:*

*I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;*

*II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.*

Ademais, a própria conceituação prevista no artigo 5º da Lei também considera este raciocínio:

*Art. 5º Para os fins desta Lei, considera-se:*

*[...]*

*VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;*

Nesse sentido, a avaliação deste artigo aliada à teoria clássica de responsabilidade civil prevista no Código Civil conduz à conclusão de que o Controlador responde por culpa *in eligendo*, ou seja, responde pela escolha de seus operadores.

No caso concreto, a presente contratação busca justamente a escolha, pelo Sesc na condição de Controlador, de um fornecedor para atuar como seu Operador.

Portanto, considerados os princípios gerais de licitação, jungido às regras de proteção e dados pessoais imposta aos Controladores pela LGPD, deve o Sesc exigir dos licitantes no edital, e não de outras partes relacionadas, as certificações de segurança da informação e controle interno de privacidade que vão assegurar o correto cumprimento do objeto contratual. Logo, diferente do que foi afirmado pelo impugnante, as exigências técnicas previstas em edital (certificações) estão corretamente colocadas.

A exigência da certificação SOC 2 não só fortalece a posição do Sesc em Minas em garantir a segurança e a privacidade dos dados de seus usuários, mas também assegura que a empresa contratada esteja alinhada com os



mais altos padrões de confiança e transparência reconhecidos internacionalmente. Esses benefícios são fundamentais para mitigar riscos e garantir que o serviço prestado seja de alta qualidade e confiabilidade (...)

Ante tais considerações, entendemos que não há ilegalidade no Edital, mantendo o entendimento contido no atual instrumento convocatório.

#### **4 – DA DECISÃO**

Isto posto, **CONHEÇO** da impugnação apresentada, e no mérito **NEGO-LHE PROVIMENTO**, desse modo, mantendo o referido edital inalterado.

**Camila Barbosa de Souza**  
**Comissão Permanente de Licitação do Sesc em Minas**