Prefeitura da Cidade do Rio de Janeiro
Secretaria Municipal de Transportes - SMTR

CONCORRÊNCIA CO SMTR Nº 001/2022
Licitação Sistema de Bilhetagem Digital

ANEXO I.9
CRITÉRIOS PARA AUDITORIA INDEPENDENTE

24 de fevereiro de 2022

ÍNDICE

ANEXO I.9 - CRITÉRIOS PARA AUDITORIA INDEPENDENTE

1. DISPOSIÇÕES GERAIS

Considera-se AUDITORIA INDEPENDENTE a empresa responsável por auxiliar o PODER CONCEDENTE na auditoria e fiscalização dos processos de segurança, modelos de negócios e funcionalidades previstas no CONTRATO de CONCESSÃO do SBD.

A AUDITORIA INDEPENDENTE constitui-se em pessoa jurídica de direito privado que comprove total independência e imparcialidade face à CONCESSIONÁRIA e ao PODER CONCEDENTE.

A AUDITORIA INDEPENDENTE será selecionada pelo PODER CONCEDENTE e contratado, sob o regime privado, pela CONCESSIONÁRIA, a quem competirá arcar, integralmente, com os respectivos custos da contratação. A contratação da AUDITORIA INDEPENDENTE deverá observar as diretrizes indicadas no corpo deste ANEXO e no CONTRATO de CONCESSÃO.

A atuação da AUDITORIA INDEPENDENTE será por tempo certo e determinado. O trabalho da AUDITORIA INDEPENDENTE deve ser desenvolvido em parceria com o PODER CONCEDENTE e a CONCESSIONÁRIA, promovendo a integração das equipes e alinhamento em relação às melhores práticas a serem adotadas.

2. CONTRATAÇÃO DA AUDITORIA INDEPENDENTE

A CONCESSIONÁRIA deverá apresentar, para prévia homologação do PODER CONCEDENTE, no prazo de 90 (noventa) dias antes do início da prestação do serviço de AUDITORIA INDEPENDENTE, ao menos 4 (quatro) empresas ou consórcios de empresas que reúnam as condições mínimas de qualificação para atuar como AUDITORIA INDEPENDENTE, conforme descrito nesta seção.

As empresas ou consórcios deverão atender aos seguintes requisitos:

i. Ter pelo menos 5 (cinco) anos de experiência no objeto;
ii. Ter comprovadamente executado serviços de características semelhantes aos descritos neste item, assim entendidos como atividades de: (i) verificação / auditoria; (ii) gerenciamento; (iii) supervisão; (iv) fiscalização e controle.
    a. As atividades deverão ser comprovadas em serviços de auditoria de processos de segurança de sistema.
    b. A comprovação de que trata esta alínea se dará obrigatoriamente em, no mínimo, duas das atividades listadas acima.
iii. Apresentar plano de trabalho demonstrando a metodologia a ser aplicada na condução dos trabalhos de acompanhamento das atividades da CONCESSIONÁRIA e seus contratados;
iv. Contar com equipe técnica de especialistas de nível superior, qualificados profissionalmente.
v. Preferencialmente, ser do grupo “Big Four", grupo das quatro maiores empresas especializadas em auditoria e consultoria do mundo, ou comprovadamente empresa com ampla experiência nesse tipo de atividade.
vi. Não poderão ser contratadas como AUDITORIA INDEPENDENTE as seguintes pessoas jurídicas e ou consórcios:
    a. Não ser CONTROLADOR DA SOCIEDADE, controlada ou coligada da CONCESSIONÁRIA ou de seus acionistas;
    b. Não estar submetida a liquidação, intervenção ou Regime de Administração Especial Temporária - RAET, falência ou recuperação judicial; não encontrar-se em cumprimento de pena de suspensão temporária de participação em licitação ou impedimento de contratar com a Administração; não ter sido declarada inidônea para licitar ou contratar com a Administração Pública, bem como não ter sido condenada, por sentença transitada em julgado, a pena de interdição de direitos devido à prática de crimes ambientais, conforme disciplinado no art. 10 da Lei n°9.605, de 12.02.1998;
    c. Impedidas ou suspensas de contratar com a Administração Pública;
    d. Cujos sócios tenham participação direta ou indireta na administração ou no quadro societário da CONCESSIONÁRIA;
    e. Que possuam contrato vigente com a CONCESSIONÁRIA, ainda que com objeto diverso; e
    f. Que, de alguma forma, possam ter sua independência e imparcialidade comprometidas.

As propostas entregues pelas empresas pré-selecionadas serão avaliadas pelo PODER CONCEDENTE. A avaliação e seleção da proposta dos participantes do processo será realizada observando cumulativamente aos seguintes critérios:

i. Atendimento aos parâmetros estabelecidos neste ANEXO;

ii. Preço compatível com o mercado;
iii. Experiência e qualificação compatível com o objeto do CONTRATO. O PODER CONCEDENTE poderá, a seu critério e a qualquer tempo:
    a. Solicitar das participantes da seleção informações adicionais para retificar ou complementar sua proposta; e
    b. Excluir da seleção empresas que possivelmente tenham interesses conflituosos com a prestação dos serviços, de modo a comprometer sua independência e imparcialidade.

O PODER CONCEDENTE se manifestará, no prazo máximo de 10 (dez) dias úteis, acerca da adequação das empresas ou consórcios de empresas apresentados pela CONCESSIONÁRIA, cabendo à CONCESSIONÁRIA formalizar, no prazo máximo de 30 (trinta) dias antes do início da prestação do serviço a contratação de uma entre as homologadas pelo PODER CONCEDENTE, para atuar como AUDITORIA INDEPENDENTE.

Observados os requisitos e impedimentos referidos previstos neste ANEXO, a equipe da AUDITORIA INDEPENDENTE deverá contar com especialistas de nível superior em todas as áreas de conhecimento relevantes para o desempenho das atribuições elencadas neste ANEXO, devendo ainda ter à disposição e mobilizar, se necessário, especialistas para apresentação de parecer relativo a questões surgidas durante a execução do CONTRATO que exijam esse tipo de análise.

Dentre os profissionais indicados para compor a equipe técnica da AUDITORIA INDEPENDENTE, deverão necessariamente estar relacionados técnicos devidamente qualificados profissionalmente com as devidas certificações para emissão de relatórios e laudos técnicos de aferição do cumprimento das diretrizes constantes ANEXO, do CONTRATO e do ANEXO I.2 - TERMO DE REFERÊNCIA.

Caso a CONCESSIONÁRIA não contrate a AUDITORIA INDEPENDENTE homologada pelo PODER CONCEDENTE ou não atenda aos prazos estabelecidos para tanto, a mesma estará sujeita às penalidades previstas no CONTRATO de CONCESSÃO.

O contrato a ser celebrado entre a CONCESSIONÁRIA e a AUDITORIA INDEPENDENTE não poderá exceder o prazo de vigência de 1 (um) ano e, sempre que houver disponibilidade no mercado, deverá ser promovida a rotatividade entre a empresa e os profissionais a serem contratados.

Quando da contratação da AUDITORIA INDEPENDENTE, a CONCESSIONÁRIA fará constar no contrato a obrigação do verificador atender integralmente ao disposto no CONTRATO de CONCESSÃO e no ANEXO I.2 - TERMO DE REFERÊNCIA.

3. ATRIBUIÇÕES DA AUDITORIA INDEPENDENTE

A fiscalização do cumprimento das obrigações da CONCESSIONÁRIA quanto aos SERVIÇOS prestados conforme o ANEXO I.2 - TERMO DE REFERÊNCIA serão realizadas pela AUDITORIA INDEPENDENTE, a quem caberá, entre outras obrigações a serem definidas pelo PODER CONCEDENTE quando da contratação, as seguintes:

1. Avaliação das Regras de Negócio do SBD;
2. Avaliação dos Processos de Segurança do SBD;

Ao final do trabalho, a AUDITORIA INDEPENDENTE deverá apresentar um parecer técnico com as informações verificadas e com a emissão de determinações. As determinações homologadas pelo PODER CONCEDENTE serão imediatamente aplicáveis e vincularão a CONCESSIONÁRIA, sem prejuízo do recurso eventualmente cabível.

A não regularização das faltas ou defeitos indicados, no prazo de 60 (sessenta) dias, que poderá ser prorrogado mediante justificativa aceita pelo PODER CONCEDENTE e sem prejuízo à continuidade e adequação dos SERVIÇOS, configura infração contratual e ensejará a lavratura de auto de infração, sujeitando a CONCESSIONÁRIA à aplicação das penalidades previstas no CONTRATO, sem prejuízo de eventual sanção administrativa, civil ou criminal por violação de preceito legal ou infralegal aplicável.

A CONCESSIONÁRIA garantirá ao PODER CONCEDENTE e a AUDITORIA INDEPENDENTE acesso irrestrito, ininterrupto e online aos sistemas de acompanhamento e monitoramento dos SERVIÇOS.

3.1. AVALIAÇÃO DAS REGRAS DE NEGÓCIO DO SBD

A Auditoria Independente deverá analisar e apresentar um relatório com as seguintes atividades:

i. Identificar as regras de negócios do SBD da CONCESSIONÁRIA;
ii. Validar os dados de entrada, com base em regras definidas e ponto de controles existentes e implementados que possam garantir a exatidão e totalidade das informações inseridas no SBD;
iii. Garantir a existência de controles que garantam a integridade das informações entre a troca de mensagens e atualização de interfaces entre o SBD, eventuais sistemas intermediários e VALIDADORES;
iv. Validar os dados de saída, com base em regras definidas e ponto de controles existentes e implementados que possam garantir a exatidão e totalidade das informações inseridas no SBD;
v. Avaliar o processo de operacionalização da Política TARIFÁRIA pelo SBD, considerando a identificação dos processos existentes e estudo do

processo de validação e aplicação de regras de negócio, contendo o mapeamento desde a origem da informação até a geração dos créditos conforme os modais estabelecidos;

vi. Identificar os controles que permitam identificar a eventual utilização anormal, distorções ou divergências, suas características e mecanismos de mitigação;

vii. Identificar os riscos associados ao processo levantado, os pontos de vistas de negócio e o ambiente tecnológico, verificando controles implementados no processo levantado, se os mesmos são efetivos e se há um plano de tratamento e contingência para os riscos mapeados;

viii. Verificar a autenticidade das assinaturas de todas as transações realizadas nas bases de dados protegidas contra modificações não autorizadas nos diversos níveis de autorização, conforme item 6.3 - Processos de Segurança do ANEXO I.2 - TERMO DE REFERÊNCIA;

ix. Realizar auditoria das transações de venda e utilização de créditos de transporte coletadas e processadas pelo SBD, por meio da verificação de registros anômalos, incluindo, mas não se limitando a:

   a. MÍDIAS cuja origem dos créditos seja desconhecida;
   b. Transações de integração tarifária sem correspondências, sem haver processamento pendente;
   c. MÍDIAS cujo montante de utilizações esteja além dos créditos nele disponíveis;
   d. Utilização de cartões bloqueados, caso sejam utilizado um Sistema baseado em CARTÕES MOEDEIROS.

x. Verificar a integridade de todos os processos realizados pelo SBD, como por exemplo, a consistência do saldo de uma CONTA DO USUÁRIO através de suas movimentações de débitos e créditos.

xi. Verificar se as rotinas de auditoria estão registrando todas as atividades importantes do SBD, como por exemplo:

   a. Registro de atividades relevantes, isto é, quaisquer atividades que possam potencialmente estar relacionadas com algum tipo de ataque.
   b. O esquema de auditoria deverá causar o menor impacto possível sobre as rotinas normais do SBD, não comprometendo desempenho e disponibilidade.
   c. A informação de auditoria deverá ser armazenada de maneira uniforme e com facilidade de acesso na consulta e interpretação, com prazo de retenção durante toda a vigência da CONCESSÃO;
   d. A informação de auditoria deverá ser protegida contra ataques.
   e. A identificação e a autenticação estão relacionadas às rotinas de auditoria. O SBD deverá ser capaz de identificar corretamente a entidade responsável pela operação registrada.

xii. Realizar auditoria e validar as informações produzidas pela CONCESSIONÁRIA e exibidas em *dashboards* para fins de cálculos dos indicadores de desempenho;
xiii. Avaliar a atribuição dos pesos dos indicadores de desempenho e propor melhorias;
xiv. Realizar auditoria e validar todos os cálculos e repasses realizados pela CONCESSIONÁRIA para a CÂMARA DE COMPENSAÇÃO TARIFÁRIA do PODER CONCEDENTE;
xv. Realizar auditoria e validar se o Plano de Conformidade com a LGPD está sendo executado em total conformidade com a Lei Geral de Proteção de Dados e com as diretrizes da ANPD, inclusive, mas não se limitando à ANONIMIZAÇÃO dos DADOS PESSOAIS, termos de CONSENTIMENTO e direitos de revogação e esquecimento;
xvi. Analisar a usabilidade do SBD e sugerir melhorias;
xvii. Analisar a documentação existente do SBD, em nível de usuários que acessam o sistema;
xviii. Identificar outras possíveis falhas e sugerir melhorias;

3.2. AVALIAÇÃO DOS PROCESSOS DE SEGURANÇA DO SBD

A AUDITORIA INDEPENDENTE deverá avaliar a segurança relacionada ao ambiente tecnológico em que o SBD se encontra em operação, considerando os processos, infraestrutura, interfaces, comunicação de dados e sistema de tecnologia da informação e comunicação, tendo por escopo as seguintes atividades:

i. **Organização da segurança de informação existente**, incluindo: estrutura, políticas, normas e procedimentos;
ii. **Segurança física e do ambiente**, em especial os controles de entrada e saída física, proteção contra ameaças externas e do meio ambiente e segurança de equipamentos;
iii. **Gerenciamento das operações e comunicações**: procedimentos e responsabilidades operacionais, documentações dos procedimentos de operação, gestão de mudanças, segregação de funções, separação dos recursos de desenvolvimento, teste e de produção, gerenciamento de serviços terceirizados, cópias de segurança, gerenciamento da segurança em rede e políticas/procedimentos para troca de informações e monitoramento;
iv. **Controle de acesso lógico de todos os sistemas envolvidos**: requisitos de negócios para controle de acesso, gerenciamento controle de acesso às redes de dados envolvidas, política de uso de serviços de rede, autenticação para conexão externo do usuário, proteção e configuração de portas de diagnóstico remotas, segregação de redes, controle de conexão de rede, controle de roteamento de redes, procedimentos seguros de entrada no sistema, identificação, autenticação de usuário; sistema de gerenciamento de senha; desconexão de terminal por inatividade; controle de acesso à aplicação, à informação; restrição de acesso à informação;

v. **Gestão de incidentes de segurança da informação**: fornecer o atendimento tempestivo aos chamados de incidentes de segurança da informação, através de uma solução de contorno ou reparo rápido e , dessa forma, minimizar o impacto no negócio ocasionado pela indisponibilidade do serviço afetado;
vi. **Desenvolvimento e manutenção de sistemas de informação,** verificando a adoção do o ciclo de desenvolvimento de software seguro (utilização de técnicas para proteger a aplicação de vulnerabilidades durante o desenvolvimento);
vii. **Gestão da continuidade do negócio**: aspectos relativos à segurança da informação (procedimentos para proteger os processos críticos contra efeito de falha ou desastres significativos, e assegurar a sua retomada em tempo hábil); e continuidade de negócios, análise/avaliação de riscos (se a gestão da continuidade de negócios inclui controles para identificar e reduzir riscos, em complementação ao processo de análise/avaliação de riscos global, limitando as consequências aos danos de incidentes e garantindo que as informações requeridas para os processos do negócio estejam prontamente disponíveis);
viii. **Testes de intrusão em infraestrutura e aplicações envolvidas**;
ix. **Avaliar os ambientes e meios físicos onde os diversos componentes do SBD estão dispostos**;
x. **Avaliar as redes de comunicação quanto à integridade, disponibilidade e confidencialidade entre os ambientes e meios físicos**;
xi. **Avaliar a segurança dos cartões utilizados nos VALIDADORES**, em especial quanto à qualidade das chaves de segurança utilizadas e à possibilidade de sua violação, caso seja adotado um Sistema Baseado em CARTÕES MOEDEIROS;
xii. **Verificar se a base denominada DATACENTER PCRJ** está sendo espelhada corretamente e em tempo real;
xiii. **Avaliar a disponibilidade média do Datacenter da CONTRATADA** com base nos logs no último ano;
xiv. **Verificar se o *site* de contigência está preparado para assumir imediatamente**, em caso de falha do *site* principal.

4. CONTRATO COM A AUDITORIA INDEPENDENTE

A CONCESSIONÁRIA deverá, na forma estabelecida no CONTRATO de CONCESSÃO, elaborar e submeter à aprovação do PODER CONCEDENTE, Termo de Referência para a contratação e Minuta de Contrato a ser celebrado com a AUDITORIA INDEPENDENTE, observadas as disposições específicas contidas no CONTRATO de CONCESSÃO. A Minuta de Contrato deverá conter, pelos menos, as seguintes disposições:

i. Objeto do CONTRATO de CONCESSÃO;
ii. Objeto da contratação em questão;
iii. Descrição detalhada das atividades a serem desenvolvidas pela AUDITORIA INDEPENDENTE;

iv. Relatórios a serem entregues e os respectivos prazos;
v. Duração do Contrato;
vi. Percentual máximo de subcontratação dos serviços;
vii. Condições de sigilo e de propriedade das informações;
viii. Relacionamento com o contratante e com o PODER CONCEDENTE.

A Minuta de Contrato deverá prever que a AUDITORIA INDEPENDENTE atuará com independência e imparcialidade. A avaliação dos serviços prestados pela AUDITORIA INDEPENDENTE por parte da Contratante se restringirá a observância dos seus aspectos formais, tais como, apresentação em formato adequado, no prazo determinado, subscrito por pessoa competente, dentre outros. Eventuais discordâncias quanto ao conteúdo produzido pela AUDITORIA INDEPENDENTE serão dirimidas no âmbito do CONTRATO de CONCESSÃO, mediante arbitragem ou peritagem, se for o caso, não ensejando a aplicação de qualquer penalidade contratual, nem tão pouco o desqualificará à continuidade da prestação dos serviços.

A formalização do contrato entre a CONCESSIONÁRIA e a AUDITORIA INDEPENDENTE e de eventuais aditivos dependerá da aprovação prévia do PODER CONCEDENTE o qual figurará como interveniente e anuente do contrato.

5. RELAÇÃO COM AS PARTES

A fim de conferir independência técnica das análises e conteúdos produzidos pela AUDITORIA INDEPENDENTE:

i. Todos os documentos, relatórios, manuais, análises e estudos produzidos pela AUDITORIA INDEPENDENTE, ainda que em versões preliminares, deverão ser produzidos em duas vias e entregues, concomitantemente, à CONCESSIONÁRIA e ao PODER CONCEDENTE.
ii. Para aqueles serviços em que a AUDITORIA INDEPENDENTE atuará mediante demanda, tanto a CONCESSIONÁRIA, quanto o PODER CONCEDENTE poderão requerer formalmente sua prestação, devendo a AUDITORIA INDEPENDENTE cientificar a outra PARTE de imediato.
iii. A AUDITORIA INDEPENDENTE goza de total independência técnica para realização dos serviços ora contratados, sendo que eventuais discordâncias quanto ao conteúdo do seu trabalho não ensejará a aplicação de quaisquer penalidades, atrasos ou descontos sobre sua remuneração.
iv. Eventuais discordâncias em relação ao conteúdo dos produtos conferidos pela AUDITORIA INDEPENDENTE, quer sejam por parte da CONCESSIONÁRIA, quer pelo PODER CONCEDENTE, serão dirimidas conforme disposições previstas no CONTRATO de CONCESSÃO.
v. Tanto CONCESSIONÁRIA quanto PODER CONCEDENTE deverão indicar uma comissão para acompanhamento da AUDITORIA INDEPENDENTE.

6. PRODUTOS DA AUDITORIA INDEPENDENTE

A AUDITORIA INDEPENDENTE deverá apresentar plano de trabalho demonstrando a metodologia a ser aplicada na condução dos trabalhos de acompanhamento das atividades da CONCESSIONÁRIA e seus contratados, além de cronograma, ponto de validação de produtos e o prazo da duração do trabalho. Deverá apresentar relatório detalhado com os resultados dos trabalhos realizados e, sempre que couber, conterá as seguintes informações:

i. Confrontação dos resultados apurados com aqueles produzidos pela CONCESSIONÁRIA e apontamento de possíveis causas para as divergências;
ii. Fontes das informações e dados utilizados no relatório;
iii. Memórias de cálculo;
iv. Indicação de procedimentos para melhorar o acompanhamento e a fiscalização do CONTRATO de CONCESSÃO;
v. Indicação de falhas porventura cometidas pelo CONCESSIONÁRIO;
vi. Nome da empresa e equipe técnica responsável pela confecção do relatório; e
vii. Outras informações que entender relevantes.

A AUDITORIA INDEPENDENTE apresentará ao PODER CONCEDENTE relatório periódico do andamento dos trabalhos de operação, devendo também, a qualquer tempo, fazer comunicações ou relatórios extraordinários referentes a quaisquer eventos relevantes. A AUDITORIA INDEPENDENTE deverá realizar reuniões periódicas de acompanhamento e controle com o PODER CONCEDENTE, registrando em ata as providências a serem adotadas no sentido de se assegurar o cumprimento das exigências e prazos do CONTRATO de CONCESSÃO, devendo o CONCESSIONÁRIO ser informado da agenda prevista para tais reuniões e receber cópia de suas atas.