PREGÃO ELETRÔNICO Nº 028/22

EXPEDIENTE Nº 0238/22

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO E INTEGRAÇÃO EM PLATAFORMA ÚNICA DE SOLUÇÃO DE GESTÃO DE SEGURANÇA DE DADOS, EM ATENDIMENTO A LEI 13709/18 - LEI GERAL DE PROTEÇÃO DE DADOS - LGPD, INCLUINDO SUPORTE TÉCNICO, GARANTIA E MANUTENÇÃO DE VERSÕES, OPERAÇÃO ASSISTIDA, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, TREINAMENTO, INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS PARA ATENDER ÀS DEMANDAS DA CET PELO PERÍODO DE 24 (VINTE E QUATRO) MESES.

CONTRATO Nº 073/2022

ÍNDICE

CONTRATO Nº 073/2022, CELEBRADO ENTRE A COMPANHIA DE ENGENHARIA DE TRÁFEGO - CET E A EMPRESA ARS TECNOLOGIA SERVICOS E CONSULTORIA LTDA.

A **COMPANHIA DE ENGENHARIA DE TRÁFEGO - CET**, com sede nesta Capital na Rua Barão de Itapetininga nº 18, inscrita no CNPJ sob o nº 47.902.648/0001-17, neste ato representada por seus Representantes Legais ao final assinados, doravante designada **CET** e a empresa **ARS TECNOLOGIA SERVICOS E CONSULTORIA LTDA** com sede nesta Capital, na rua do Rocio nº 220, Vila Olímpia, CEP 04.552-903, com telefone nº (11) 3044-1819 e e-mail: licitacao@neotel.com.br, inscrita no CNPJ sob o nº 04.189.909/0001-90 e Inscrição Estadual nº 145.402.048.113, neste ato representada por seu(s) Representante(s) Legal(is) ao final assinado(s), doravante designada **CONTRATADA**, têm entre si justo e contratado o seguinte:

CLÁUSULA PRIMEIRA - OBJETO CONTRATUAL, DESCRIÇÃO DA SOLUÇÃO E REQUISITOS TÉCNICOS E FUNCIONAIS

1.1. Constitui objeto deste Contrato, pelo regime de empreitada por preço unitário, a prestação de serviços de segurança da informação e integração em plataforma única de solução de gestão de segurança de dados, em atendimento a Lei Geral de Proteção de Dados nº 13.709/18 (LGPD), incluindo suporte técnico, garantia e manutenção de versões, operação assistida, serviços de instalação e configuração da solução, treinamento, integrações necessárias com soluções de terceiros para atender às demandas da **CET**, obrigando-se a **CONTRATADA** a executá-lo de acordo com o **PREGÃO ELETRÔNICO Nº 028/22**, com o Anexo I - Termo de Referência, com o Anexo II - Proposta e demais elementos que compõe o expediente mencionado no preâmbulo, os quais passam a integrar este instrumento.

1.2. A descrição da solução e os requisitos técnicos e funcionais estão dispostos nos itens 3 e 5 do Anexo I - Termo de Referência

CLÁUSULA SEGUNDA - VIGÊNCIA, PRAZOS E LOCAL DE ENTREGA/PRESTAÇÃO DOS SERVIÇOS

2.1. O prazo de duração deste Contrato é de 24 (vinte e quatro) meses, contados a partir data da sua assinatura, podendo ser prorrogado sucessivamente em prazo inferior ou igual ao contrato inicial, até o limite legal.

2.2. O prazo máximo de entrega de todos os hardwares/softwares que compõem a solução serão de 60 (sessenta) dias corridos, contados a partir da data de abertura de ordem de serviço.

2.3. O prazo máximo para Instalação e configuração (implementação) da solução será de 90 (noventa) dias corridos contados a partir da entrega dos equipamentos, devendo obrigatoriamente ser realizada em finais de semana ou feriados, conforme agendamento da CET.

2.4. O local para a prestação dos serviços e para a entrega do objeto deste Edital, será na Gerencia de Informática da **CET** localizado na Rua Bela Cintra nº 385 - 2º andar - Bairro Centro - São Paulo/SP, de segunda a sexta-feira das 08h00 às 17h00.

2.4.1. As licenças deverão ser disponibilizadas através de arquivo e/ou chave de licenciamento disponibilizado pelo fabricante nomeados ao cliente final, e com os respectivos números de série. Quando da disponibilização das licenças, deverão ser entregues os aplicativos instaladores (executáveis/binários) acompanhados de documentação técnica em formato digital (manuais de operação) de cada software que compõe a solução, conforme item 19.2 do Anexo I - Termo de Referência.

CLÁUSULA TERCEIRA - CONDIÇÕES DE IMPLEMENTAÇÃO DOS SERVIÇOS

3.1. As condições de prestação destes serviços está disposta no item 10 do Anexo I - Termo de Referência.

CLÁUSULA QUARTA - OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

4.1. As principais Obrigações e Responsabilidades da **CONTRATADA** estão dispostas no item 11 do Anexo I - Termo de Referência, além delas, a **CONTRATADA** deverá:

4.1.1. Indicar seu preposto em até 05 (cinco) dias, contados a partir da data da assinatura deste Instrumento, para representá-la na execução deste Contrato, informando e-mail e telefone para contato.

4.1.1.1. A **CONTRATADA** deverá apresentar também, em até 05 (cinco) dias, contados a partir da data da assinatura deste Instrumento, elação contendo os nomes dos empregados que trabalharão na execução deste Contrato e copias de registros dos mesmos junto a empresa, devidamente anotado na carteira de trabalho e previdência social – CTPS, por meio da sua via original ou de cópia autenticada.

4.1.2. No caso de substituição de funcionários durante a execução deste Contrato, deverá ser comunicado para o Fiscal/Gestor do Contrato da **CET**, em até 05 (cinco) dias úteis, **antes da ocorrência do fato**.

4.1.3. Manter, durante toda a execução do Contrato, em compatibilidade com as demais obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação indicada no preâmbulo deste Contrato.

4.1.4. Comparecer, sempre que convocada, pelo Gestor do Contrato ou pessoa indicada pelo mesmo, ao local designado pela **CET**, por meio de pessoa devidamente credenciada, para exame, esclarecimentos e informações de quaisquer problemas relativos aos serviços, executados ou em execução.

4.1.5. Dar ciência imediata e por escrito à **CET** sobre qualquer anormalidade que verificar na execução dos serviços.

4.1.6. Obriga-se a reparar, corrigir, ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos serviços.

CLÁUSULA QUINTA - OBRIGAÇÕES DA CET

5.1. Designar o Gestor e o Fiscal do Contrato responsável pela gestão do Contrato, a quem competirá a fiscalização dos serviços, a qualquer instante, solicitando à **CONTRATADA**, sempre que achar conveniente, informações do seu andamento, bem como pelo recebimento dos veículos.

5.2. Cumprir e exigir o cumprimento das obrigações deste Contrato e das disposições legais que a regem, Exigindo da **CONTRATADA**, a qualquer tempo, a comprovação das condições requeridas para a contratação.

5.3. Comunicar à **CONTRATADA**, no prazo máximo de 24 horas, qualquer possível irregularidade detectada quando da execução dos serviços, formulando exigências necessárias às respectivas regularizações.

5.4. Encaminhar a liberação de pagamento da fatura devidamente aprovada, referente a prestação de serviços efetuada pela **CONTRATADA**.

5.5. Aplicar as penalidades previstas neste contrato, em caso de descumprimento pela **CONTRATADA** de quaisquer cláusulas estabelecidas.

CLÁUSULA SEXTA - VALOR E PREÇO

6.1. O valor total do presente Contrato é de **R$ 13.805.480,00** (treze milhões, oitocentos e cinco mil, quatrocentos e oitenta reais), em função dos preços unitários indicados na Proposta, na data base de 09/08/2022 e do quadro a seguir:

Item	Descrição	Métrica/unidade	Quantidade	Preço Unitário R$
6.1.1.	Console de Gerenciamento de Chaves Criptográficas	Licença Perpétua / Aquisição	02	473.500,00
6.1.2.	Criptografia para Sistemas de Arquivos de Servidores	Licença Perpétua / Aquisição	11	104.130,00
6.1.3.	Criptografia de Registros em Bancos de Dados via Aplicações Web	Licença Perpétua / Aquisição	05	118.300,00
6.1.4.	Criptografia para Compartilhamento Seguro de Base de Dados	Licença Perpétua / Aquisição	01	503.400,00
6.1.5.	Módulo de Mapeamento de Classificação de dados.	Licença Subscrição (Mensalidade)	24	86.000,00
6.1.6.	Solução de gestão de identidade e acesso.	Licença Subscrição (Mensalidade)	24	128.500,00
6.1.7.	Solução de Prevenção de vazamento de dados.	Licença Subscrição (Mensalidade)	24	59.500,00
6.1.8.	Solução de gestão de credenciais de alto privilégio	Licença Perpétua / Aquisição	01	584.000,00
6.1.9.	Painel Central de Gerenciamento de Indicadores de Segurança	Licença Subscrição (Mensalidade)	24	34.000,00
6.1.10.	Manutenção e Garantia de Console de Gerenciamento de Chaves Criptográficas	Serviço mensal	24	11.425,00
6.1.11.	Manutenção e Garantia para Criptografia para Sistema de Arquivos de Servidores	Serviço mensal	24	13.048,00
6.1.12.	Manutenção e Garantia para Criptografia de Registros em Bancos de Dados via Aplicações Web	Serviço mensal	24	6.250,00
6.1.13.	Manutenção e Garantia para Criptografia de Compartilhamento Seguro de Base de Dados	Serviço mensal	24	5.353,00
6.1.14.	Manutenção e Garantia para Solução de gestão de credenciais de alto privilégio	Serviço mensal	24	5.683,00
6.1.15.	Instalação e Configuração de plataforma de criptografia	Serviço	01	132.434,00

Item	Descrição	Métrica/unidade	Quantidade	Preço Unitário R$
6.1.16.	Treinamento	Serviço	01	47.000,00
6.1.17.	Serviço de Operação Assistida	Serviço mensal	23	63.500,00

6.2. O preço total para a execução dos serviços, é o constante da proposta comercial da licitante e remunerará todos os custos básicos diretos, bem como o frete, transporte, encargos sociais e trabalhistas, previdenciários, fiscais ou quaisquer outros que incidam ou venham a incidir direta ou indiretamente sobre o objeto deste Contrato.

CLÁUSULA SÉTIMA - CONDIÇÕES DE FATURAMENTO E DE PAGAMENTO

7.1. FATURAMENTO

7.1.1. Para a console de gerenciamento de chaves criptográficas, criptografia de dados para servidores, criptografia de dados via aplicação web, criptografia para compartilhamento seguro de base de dados, solução de gestão de credenciais de alto privilégio deverão ser faturados integralmente (licença perpétua) a partir da conclusão do fornecimento e instalação da solução em ambiente da **CET**.

7.1.2. Para os módulos de mapeamento e classificação de dados, solução de gestão de identidade e acesso, solução de prevenção à vazamento de dados e painel central de indicadores de segurança, deverão ser faturados mensalmente (licença mensal) a partir da conclusão do fornecimento e instalação da solução em ambiente da **CET**.

7.1.3. Deverá ser extraído da console de gerenciamento o relatório que demonstre o pleno funcionamento do equipamento e os softwares vinculados para a ação de criptografia nos cenários listados.

7.1.4. De posse do relatório deverá ser emitido por parte da **CET** termo que ateste a instalação da solução e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente à emissão do termo acima.

7.1.5. Os serviços de Suporte Técnico, Manutenção e Garantia deverão ser atestados através de relatório técnico emitido pela **CONTRATADA** e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia do mês subsequente à prestação do serviço mensal.

7.1.6. O Serviço de Operação Assistida será mensurado como um serviço mensal e deverá ser atestado através de relatório técnico emitido pela **CONTRATADA** e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia do mês subsequente à prestação do serviço;

7.1.7. O serviço de Instalação e Configuração é considerado atividade de execução única e faturado a partir da emissão do Termo de Aceite de Conclusão da Instalação e Configuração e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente à emissão do termo acima e autorização do Gestor do Contrato;

7.1.8. O valor relativo ao Treinamento será faturado a partir da emissão do Termo de Aceite de Conclusão de Treinamento e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente à emissão do termo acima e autorização do Gestor do Contrato.

7.2. PAGAMENTO

7.2. A **CONTRATADA** emitirá a Nota Fiscal Eletrônica ou documento equivalente, após o recebimento da Nota Fiscal Eletrônica de Serviços, a **CET** disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite, aprovando os serviços prestados, que será paga, no prazo de 30 (trinta) dias, contados a partir da data de emissão do Termo de Aceite.

7.2.1. Caso a Nota Fiscal Eletrônica de Serviços contenha divergências com relação ao estabelecido no Instrumento Contratual, a **CET** comunicará a **CONTRATADA**, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis devolvendo a mesma para correção.

7.2.2. 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 **CET**.

7.3. Além da Nota Fiscal Eletrônica ou documento equivalente, o pedido de pagamento deverá ser acompanhado da prova de inexistência de registro no CADIN do Município de São Paulo.

7.4. Ocorrendo eventual atraso no pagamento, por culpa da **CET**, o valor do principal devido será reajustado 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, nos termos da Portaria 5/12 da Secretaria das Finanças.

7.5. O pagamento será efetuado exclusivamente em conta corrente bancária, na Caixa Econômica Federal - CEF, indicada pela **CONTRATADA**, a informação deverá ser encaminhada para a Gerência Financeira - GFI, Rua Barão de Itapetininga nº 18 - 4º andar.

7.6. Caso a **CONTRATADA** solicite que o pagamento seja creditado em conta corrente de outro banco que não na Caixa Econômica Federal - CEF, arcará com todas as despesas e tarifas bancárias vigentes, incorridas na transação de pagamento: DOC, TED, tarifa de emissão de cheque e outras.

7.7. A **CONTRATADA** deverá encaminhar os arquivos eletrônicos para a Gerência Financeira - GFI (e.mail: gfi@cetsp.com.br) no caso de utilização da DANFE, ficando o pagamento condicionado ao encaminhamento desses arquivos.

7.8. Nenhum pagamento isentará a **CONTRATADA** das responsabilidades contratuais, nem implicará na aceitação dos serviços pela **CET**.

CLÁUSULA OITAVA - REAJUSTE

8.1. Os preços contratados somente poderão ser reajustados após um ano da data limite para apresentação da proposta, pela variação do índice IPC-FIPE, com base na Portaria SF nº 389 de 18 de dezembro de 2017, que dispõe instruções para cumprimento excepcional do artigo 7º do Decreto Municipal nº 57.580/17, observando-se as demais normas que regulamentam a matéria.

8.2. As condições de reajustamento ora pactuadas poderão ser alteradas em face da superveniência de normas federais ou municipais aplicáveis à espécie.

CLÁUSULA NONA - IMPOSTOS E INCIDÊNCIAS FISCAIS

9.1. Os tributos, taxas, impostos, emolumentos, contribuições previdenciárias, trabalhistas, fiscais e parafiscais que sejam devidos em decorrência, direta ou indireta, deste Contrato, serão de exclusiva responsabilidade da **CONTRATADA**, assim definido na legislação vigente, sem direito a reembolso.

CLÁUSULA DÉCIMA - GARANTIA DE EXECUÇÃO CONTRATUAL

10.1. A **CONTRATADA** deverá apresentar à **CET** a Garantia de Execução Contratual, no valor de **R$ 414.164,40** (quatrocentos e quatorze mil, cento e sessenta e quatro reais e quarenta centavos), correspondente a 3% (três por cento) do valor total do presente Contrato, no prazo de até 10 (dez) dias corridos após a celebração do respectivo instrumento, sob pena de aplicação de multa, a fim de assegurar a sua execução e será prestada em qualquer das modalidades admitidas pelo § 1º do artigo 70 da Lei Federal nº 13.303/16 e § 1º do artigo 141 Regulamento Interno de Licitações, Contratos e Convênios - RILCC, regulamentada pela Portaria nº 122/09, da Secretaria de Finanças do Município de São Paulo.

10.1.1. A multa referida na cláusula anterior correspondente a até 0,01% (zero virgula zero um por cento) por dia de atraso, do valor total do contrato, conforme inciso IV do artigo 193, do Regulamento Interno de Licitações, Contratos e Convênios - RILCC.

10.1.2. Em caso da **CONTRATADA** optar pela prestação da Garantia na modalidade de Fiança Bancária, deverá apresentar conforme o Anexo VIII - Modelo de Fiança Bancária, do Edital.

10.1.3. O prazo para a apresentação da garantia poderá ser prorrogável mediante solicitação e apresentação de justificativas a serem submetidas a apreciação pela CET.

10.2. A não apresentação da garantia, prevista na cláusula anterior, em até 20 (vinte) dias úteis, autorizará a rescisão unilateral do contrato por descumprimento ou cumprimento irregular de suas cláusulas.

10.3. A garantia será devolvida à **CONTRATADA** em até 30 (trinta) dias da lavratura do Termo de Recebimento Definitivo do objeto e após a quitação das multas contratuais eventualmente existentes, atualizada monetariamente nos termos § 4º do artigo 141 do Regulamento Interno de Licitações, Contratos e Convênios - RILCC.

10.4. Se houver prorrogação ou acréscimo ao valor do Contrato, a **CONTRATADA** se obriga a fazer a complementação da garantia na assinatura do respectivo Termo Aditivo, ou excepcionalmente, no prazo máximo de 10 (dez) dias úteis, contados da data de assinatura do respectivo Termo Aditivo.

CLÁUSULA DÉCIMA PRIMEIRA - TREINAMENTO

11.1. As condições de prestação destes serviços estão dispostas no item 16 do Anexo I - Termo de Referência.

CLÁUSULA DÉCIMA SEGUNDA - SUPORTE TÉCNICO, OPERAÇÃO ASSISTIDA, MANUTENÇÃO E GARANTIA DA SOLUÇÃO

12.1. As condições de prestação destes serviços estão dispostas nos itens 8, 9 e 11 do Anexo I - Termo de Referência.

CLÁUSULA DÉCIMA TERCEIRA - PENALIDADES

13.1. Pelo descumprimento das obrigações assumidas a **CONTRATADA** estará sujeita às penalidades previstas no Capítulo II, Seção III, artigo 82 da Lei Federal nº 13.303/16 e Capítulo XIII do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da **CET**, garantindo a prévia defesa, estando sujeita ainda às seguintes multas/sanções, cujo cálculo tomará por base o valor do Contrato nas mesmas bases do ajuste:

13.1.1. **ADVERTÊNCIA**, para os casos de descumprimento dos itens 6.1; 6.2; 9.2; 9.3. e 11.5. do Anexo I – Termo de Referência. A aplicação da advertência deverá ser comunicada por correspondência escrita, mesmo que registrada da forma eletrônica ou em atas de reunião, devendo ocorrer seu registro junto ao Cadastro Corporativo da **CET**, independentemente da **CONTRATADA** ser ou não cadastrada.

13.1.2. Havendo reincidência da sanção de advertência, incorrerá à **CONTRATADA** em multa de 1,0% (um por cento) do valor referente ao mês da infração, valor esse que será descontado no ato do pagamento da Nota Fiscal ou Fatura, após a comunicação da irregularidade pela **CET** à **CONTRATADA** e observada a ampla defesa;

13.1.3. Caso a **CONTRATADA** não atenda ao prazo estipulado nos itens 2.2, 2.3 e 4.1.1.1. deste Contrato e item 10.2.10.8.4. do Anexo I - Termo de Referência, incidirá multa diária de 5% (cinco por cento), calculado sobre o valor contratual mensal referente ao mês da infração. Após 05 (cinco) dias corridos de descumprimento estará caracterizada inexecução parcial do Contrato e a aplicação das penalidades inerentes.

13.1.4. Pelo não cumprimento dos prazos estipulados nos itens 11.16 e 11.18. deste Contrato, incidirá multa de 0,1% (zero virgula um por cento) por hora de atraso, calculado sobre o valor contratual mensal referente ao mês da infração. Após 05 (cinco) dias corridos de descumprimento, restará configurada inexecução parcial do Contrato e a aplicação das penalidades inerentes.

13.1.5. Multa de 1% (um por cento) sobre o valor contratual mensal referente ao mês da infração, quando, sem justa causa aceita pela **CET**, a **CONTRATADA** não cumprir com qualquer outra obrigação assumida em decorrência do Contrato.

13.1.6. Em caso de reincidência no item 13.1.5., aplicar-se Multa de 2% (dois por cento) sobre o valor contratual mensal referente ao mês da infração.

13.1.6.1. Caso a reincidência obste a execução do serviço será aplicada a pena de Inexecução Parcial.

13.2. Pelo descumprimento das condições de confidencialidade previstas na Clausula dezoito, incidirá multa de 15% (quinze por cento) do valor total do Contrato.

13.3. Pelo inadimplemento total ou parcial deste Contrato, independentemente da rescisão, a **CONTRATADA** ficará sujeita a critério da **CET** às seguintes penalidades:

13.3.1. Multa de 10% (dez por cento) sobre a parcela inexecutada, por inexecução parcial do ajuste, nos termos do Art. 193, V do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da **CET**.

13.3.2. Multa de 20% (vinte por cento) sobre o valor contratual, por inexecução total do ajuste, nos termos do Art. 193, VI do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da **CET**.

13.3.3. A inexecução parcial ou total do Contrato poderá ensejar sua rescisão nos termos do artigo nº 182 do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da **CET**.

13.3.4. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração Pública, por prazo não superior a 02 (dois) anos ou enquanto perdurarem os motivos determinantes da punição ou, ainda, até que seja promovida a reabilitação, quando houver, em especial:

a) reincidência de execução insatisfatória na prestação de serviços contratados;

b) atraso injustificado na execução/conclusão dos serviços, contrariando o disposto no contrato;

c) reincidência na aplicação das penalidades de multa;

d) irregularidades que ensejem a rescisão contratual;

e) condenação definitiva por praticar fraude fiscal no recolhimento de quaisquer tributos;

f) prática de atos ilícitos visando prejudicar a execução do contrato;

g) prática de atos ilícitos que demonstrem não possuir a Contratada idoneidade para contratar com a **CET**.

13.3.5. Declaração de inidoneidade para licitar e contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

a) A declaração de inidoneidade poderá ser proposta ao Diretor Presidente da **CET** quando constatada a má-fé, ação maliciosa e premeditada em prejuízo da **CET**, evidência de atuação com interesses escusos, inclusive apresentação de documentos falsos ou falsificados ou reincidência de faltas que acarretem prejuízos à **CET** ou aplicações sucessivas de outras penalidades.

13.3.6. A pena de multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e sua cobrança não isentará a **CONTRATADA** da obrigação de indenizar eventuais perdas e danos.

13.3.7. Eventuais penalidades pecuniárias, aplicadas à **CONTRATADA** após o devido procedimento, poderão ser ressarcidas por meio de compensação, descontando-se de pagamentos vincendos que a **CONTRATADA** tenha a receber da **CET,** relativamente a este Contrato ou, poderão ser descontados da garantia prestada, se houver ou, ainda, ser cobrado administrativa ou judicialmente.

13.3.8. Se o valor da compensação prevista no subitem **13.2.7.** for insuficiente para pagamento da(s) penalidade(s), fica a **CONTRATADA** obrigada a recolher a importância devida no prazo de 15 (quinze) dias corridos, contados a partir da comunicação oficial da **CET**.

13.3.9. A compensação citada no item **13.2.7** ficará restrita ao âmbito do presente Contrato.

13.3.10. No caso de aplicação de eventuais penalidades, será observado o procedimento previsto no Regulamento Interno de Licitações, Contratos e Convênios - RILCC da **CET**.

13.3.11. Será remetida à Secretaria Municipal de Gestão - Seção de Cadastro de Fornecedores, cópia do ato que aplicar qualquer penalidade ou da decisão final do recurso interposto pela **CONTRATADA**, a fim de que seja averbada a penalização no cadastro municipal de fornecedores.

13.3.12. As sanções/multas são independentes e a aplicação de uma não exclui a das outras, sendo descontadas do pagamento respectivo ou, se for o caso, cobradas administrativa ou judicialmente.

13.3.13. A fixação dos percentuais de multa previstos nesta cláusula, em percentuais inferiores aos limites indicados, poderá ser definida a critério da autoridade competente, por despacho fundamentado, com base em relato circunstanciado da área **CET** gestora da contratação.

CLÁUSULA DÉCIMA QUARTA - SUBCONTRATAÇÃO

14.1. A **CONTRATADA** poderá subcontratar, desde que haja prévia e expressa autorização da **CET**, sob pena de rescisão do Contrato e das sanções previstas na Lei Federal nº 13.303/16, apenas nas condições a seguir:

14.1.1. O sistema operacional poderá ser desenvolvido a partir de melhoramentos em códigos previamente existentes, até o limite de 30% do sistema;

14.2. Permanecem sob a responsabilidade da **CONTRATADA** todos os serviços executados, independentemente da autorização da subcontratação por parte da **CET**.

14.3. A **CONTRATADA**, sem prejuízo das suas responsabilidades contratuais e legais, será a única responsável pelos serviços executados pela **SUBCONTRATADA**, sob pena de rescisão deste Contrato e sem prejuízo de outras penalidades cabíveis.

CLÁUSULA DÉCIMA QUINTA - RESCISÃO

15.1. Constituem motivo para rescisão de contrato, dentre outros:

I - o não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

II - a alteração da pessoa do contratado, mediante:

a) A subcontratação total do seu objeto, a associação do contratado com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, sem anuência da CET

III - o desatendimento das determinações regulares da **CET** decorrentes do acompanhamento e fiscalização do contrato;

IV - o cometimento reiterado de faltas na execução contratual;

V - a dissolução da sociedade ou o falecimento do contratado;

VI - a decretação de falência ou a insolvência civil do contratado;

VII - a alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;

VIII - razões de interesse da **CET**, de alta relevância e amplo conhecimento, justificadas e exaradas no processo administrativo;

IX - o atraso nos pagamentos devidos pela **CET** decorrentes de obras, serviços ou fornecimentos, ou parcelas destes, já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

X - a não liberação, por parte da **CET**, de área, local ou objeto para execução de obra, serviço ou fornecimento, nos prazos contratuais, bem como das fontes de materiais naturais especificadas no projeto;

XI - a ocorrência de caso fortuito, força maior ou fato do príncipe, regularmente comprovada, impeditiva da execução do contrato;

XII - a não integralização da garantia de execução contratual no prazo estipulado;

XIII - o descumprimento da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;

XIV - o perecimento do objeto contratual, tornando impossível o prosseguimento da execução da avença;

XV - ter frustrado ou fraudado, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público; ter impedido, perturbado ou fraudado a realização de qualquer ato de procedimento licitatório público; ter afastado ou procurado afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; ter fraudado licitação pública ou contrato dela decorrente; ter criado, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo; ter obtido vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ter manipulado ou fraudado o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública; ter dificultado atividade de investigação ou fiscalização de

órgãos, entidades ou agentes públicos, ou ter intervindo em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização.

15.2. As práticas passíveis de rescisão, tratadas nesse inciso, podem ser definidas, dentre outras, como:

a) corrupta: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação do empregado da **CET** na execução do contrato;

b) fraudulenta: falsificar ou omitir fatos, com o objetivo de influenciar o processo de execução do contrato;

c) coercitiva: causar dano ou ameaçar, direta ou indiretamente, as pessoas físicas ou jurídicas, visando afetar a execução do contrato;

d) obstrutiva: destruir, falsificar, alterar ou ocultar provas ou fazer declarações falsas, com objetivo de impedir materialmente a apuração de práticas ilícitas.

15.3. As práticas exemplificadas no subitem **15.2.**, além de acarretarem responsabilidade administrativa, a ser apurada no curso do próprio processo administrativo de contratação, de acordo com o caso concreto, poderão implicar em responsabilidade civil indenizatória e/ou indenização na esfera criminal, nos termos da Lei.

15.4. Os casos de rescisão contratual devem ser formalmente motivados nos autos do processo, devendo ser assegurado o contraditório e o direito de prévia e ampla defesa.

CLÁUSULA DÉCIMA SEXTA - RECEBIMENTO DO OBJETO

16.1. Após a instalação e configuração da solução, a equipe técnica da **CET** emitirá o "Termo de Aceite de Entrega e Instalação" das licenças perpétuas em até 05 (cinco) dias úteis após a formalização pela **CONTRATADA** da finalização do processo da instalação/configuração (operação) da solução e confirmação que todos os quesitos estão sendo cumpridos conforme o Edital.

16.1.1. Entende-se pela instalação e configuração, tanto a parte física da solução, configuração lógica de todos os produtos/serviços e testes de todas as regras e procedimentos necessários a operação do serviço.

16.1.2. O objeto do Contrato somente será recebido quando perfeitamente de acordo com as condições contratuais e demais documentos que fizerem parte do ajuste.

16.2. Executado o contrato, o seu objeto deverá ser recebido:

I - em se tratando de obras e serviços:

a) provisoriamente, pelo responsável por seu acompanhamento e fiscalização; ou

b) definitivamente, pelo Gestor do Contrato.

16.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil, principalmente quanto à solidez e segurança da obra ou do serviço, nem ético profissional pela perfeita execução nos limites estabelecidos pelo Código Civil Brasileiro e pelo contrato.

16.4. Nos casos devidamente justificados, os prazos para recebimento provisório e definitivo poderão ser prorrogados mediante autorização da autoridade competente, formalizada através de Aditamento, desde que celebrado anteriormente ao término da vigência contratual.

16.5. Na hipótese de rescisão do contrato, caberá ao responsável pela fiscalização atestar as parcelas adequadamente concluídas, recebendo provisória ou definitivamente, conforme o caso.

CLÁUSULA DÉCIMA SÉTIMA - LEGISLAÇÃO APLICÁVEL

17.1. Lei Federal nº 10.520/02, Lei Federal 13.303/16, Lei Complementar n° 123/06 e suas alterações posteriores, Decreto Municipal nº 44.279/03 e Regulamento Interno de Licitações, Contratos e Convênios - RILCC da CET, aplicando-se, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

CLÁUSULA DÉCIMA OITAVA - DA MATRIZ DE RISCO

18.1. A Matriz de Risco é o instrumento tem o objetivo de definir as responsabilidades do Contratante e do Contratado na execução do contrato.

18.1.1. Constitui peça integrante deste contrato, independentemente de transcrição no instrumento respectivo, o Anexo Matriz de Risco do EDITAL

18.1.2. O termo risco foi designado neste contrato para designar o resultado objetivo da combinação entre probabilidade de ocorrência de determinado evento, aleatório, futuro e que independa da vontade humana, e o impacto resultante caso ele ocorra. Esse conceito pode ser ainda mais específico ao se classificar o risco como uma atividade de ocorrência de um determinado evento que gere provável prejuízo econômico.

18.1.3. A análise dos riscos associados a esta contratação é realizada através da matriz de risco constante no **ANEXO XII** que tem por objetivo traçar as diretrizes das cláusulas contratuais. Por isso todos os riscos são indicados na forma de Anexo do Edital e tem por objetivo refletir os eventos mitigáveis incidentes no projeto.

18.2. A responsabilidade da **CONTRATADA** e do **CONTRATANTE** estão estabelecidas na MATRIZ DE RISCO.

18.2.1. As responsabilidades são exclusivas e ilimitadas.

18.2.3. Os riscos previstos de responsabilidade da **CONTRATADA** não podem ser objeto de aditamento.

18.3. Sempre que atendidas as condições do CONTRATO e mantida as disposições da MATRIZ DE RISCO, considera-se mantido seu equilíbrio econômico-financeiro.

18.3.1. A **CONTRATADA** somente poderá solicitar a recomposição do equilíbrio econômicofinanceiro nas hipóteses excluídas de sua responsabilidade na MATRIZ DE RISCO.

CLÁUSULA DÉCIMA NONA - DISPOSIÇÕES FINAIS E CONFIDENCIALIDADE

19.1. Para 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 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 Municipal nº 56.633/15.

19.2. A **CONTRATADA** concorda com as normas, políticas e práticas estabelecidas no **Código de Conduta e Integridade da CET,** disponível no site da CET/Transparência CET, no link: http://www.cetsp.com.br/media/719911/codigo-de-conduta-e-integridade-1a-rev.pdf, comprometendo-se com o seu integral cumprimento, inclusive por parte de seus empregados e prepostos, conforme previsto na Lei Federal nº 13.303/16 e no Decreto Municipal nº 58.093/18, comprometendo-se com a ética, dignidade, decoro, zelo e 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.

19.3. A **CONTRATADA** concorda e compromete-se em cumprir as Normas de Segurança de Informações estabelecidas na CET, nos termos da Política de Segurança da Informação - PSI, disponível em http://www.cetsp.com.br/media/1177904/15-politica-de-seguranca-da-informacao-cet.pdf.

19.4. A CONTRATADA obrigar-se-á a manter a mais absoluta confidencialidade a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade da CONTRATANTE, aos quais tiver acesso em decorrência da prestação de serviços relacionados ao presente Edital, ficando terminantemente proibida de fazer uso ou revelação destes, sob qualquer justificativa.

19.5. Nenhuma tolerância das partes quanto à falta de cumprimento de quaisquer das cláusulas do ajuste poderá ser entendida como aceitação, novação ou precedente.

19.6. 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 **CET**, durante e após fim deste Contrato, salvo se houver autorização expressa da **CET** para divulgação.

19.7. 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 **CET**. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

CLÁUSULA VIGÉSIMA - FORO

20.1. Para solucionar quaisquer questões oriundas deste Contrato, é competente, por disposição legal, o foro da Fazenda Pública da Comarca da Capital, São Paulo.

E, por se acharem assim justas e contratadas, assinam o presente Contrato em 02 (duas) vias de igual teor e forma, diante das testemunhas abaixo indicadas, que também o assinam.

São Paulo, de Setembro de 2022

PELA CET

ROBERTO LUCCA MOLIN	**JAIR DE SOUZA DIAS**
Diretor Administrativo e Financeiro	**Presidente**

PELA CONTRATADA

NOME:
CPF:
RG:

Testemunhas:

CET: **CONTRATADA:**

1) **2)**
ADRIANA RAMOS DOS SANTOS
CPF:

CONTRATO Nº 073/22

PREGÃO ELETRÔNICO Nº 028/22

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO E INTEGRAÇÃO EM PLATAFORMA ÚNICA DE SOLUÇÃO DE GESTÃO DE SEGURANÇA DE DADOS, EM ATENDIMENTO A LEI 13709/18 - LEI GERAL DE PROTEÇÃO DE DADOS - LGPD, INCLUINDO SUPORTE TÉCNICO, GARANTIA E MANUTENÇÃO DE VERSÕES, OPERAÇÃO ASSISTIDA, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, TREINAMENTO, INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS PARA ATENDER ÀS DEMANDAS DA CET PELO PERÍODO DE 24 (VINTE E QUATRO) MESES.

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

A presente licitação objetiva a contratação de empresa especializada na prestação de Serviços de Segurança da Informação e Integração em Plataforma única de solução de gestão de segurança de dados, em atendimento a Lei Geral de Proteção de Dados (LGPD) – 13.709/18, conforme condições estabelecidas neste Termo de Referência e seus anexos, incluindo suporte técnico, garantia e manutenção de versões, operação assistida, serviços de instalação e configuração da solução, treinamento, integrações necessárias com soluções de terceiros para atender às demandas da Companhia de Engenharia de Tráfego – CET pelo período de 24 (vinte e quatro) meses.

2. JUTIFICATIVA

2.1 Origem e necessidade da demanda

2.1.2 A Companhia de Engenharia de Tráfego – CET, atendendo aos objetivos e às necessidades da municipalidade, possui como missão contribuir para a Mobilidade da cidade de São Paulo, por meio do estímulo e da integração dos diferentes meios de deslocamentos, visando à melhoria da qualidade de vida dos cidadãos.

2.1.3 Nesse sentido, para o alcance dos objetivos estratégicos que sustentam essa missão, é necessário compreender que há um universo multidisciplinar por trás do escopo de atividades que a CET desenvolve. Esse escopo integra, além de atividades de planejamento no trânsito, projetos sinalização viária e operação do sistema viário, uma componente de significativo impacto que tangencia a modernização tecnológica das centrais de tráfego e de toda a infraestrutura de serviços que apoiam essas atividades.

2.1.4 Essa necessidade de investimentos e dedicação de recursos ao campo da tecnologia torna-se relevante, haja vista o destaque do crescimento contínuo dos conceitos de *"Smart Cities"* e o impacto direto do aumento no uso de soluções tecnológicas após a pandemia do novo Corona Vírus, que modificou de forma sensível as necessidades, hábitos, rotinas e a relação de trabalho e de consumo ao redor do mundo, afetando, por consequência, a mobilidade da população em geral.

2.1.5 Frente à essas necessidades, a CET vem se mobilizando para conhecer e estudar estes movimentos e desafios, visando identificar novas tendências mundiais que possam afetar o tema mobilidade.

2.1.6 Corrobora este entendimento o Planejamento Estratégico publicado e elaborado para os anos de 2022 a 2026, que está diretamente vinculado ao Compromisso de Desempenho Institucional – CDI da Companhia, planejamento esse que determinou, dentre os objetivos estratégicos, a necessidade do Fortalecimento do uso da tecnologia e de instrumentos de Gestão (objetivo número III), tanto no ambiente interno da CET como em projetos a serem futuramente implementados.

n.º	Objetivos Estratégicos da CET	Temas e Metas PdM
I	MELHORAR A **SEGURANÇA VIÁRIA**, APLICANDO OS CONCEITOS "VISÃO ZERO" E "SISTEMAS SEGUROS"	- Segurança Viária - Meta 39 - Mobilidade Ativa – Metas 41 e 43 - Transporte Público – Meta 48
II	GARANTIR A **MOBILIDADE ATIVA**, INCENTIVANDO OS DESLOCAMENTOS À PÉ E DE BICICLETA E ESTIMULANDO A INTEGRAÇÃO DOS MODAIS	- Segurança Viária - Meta 39 - Mobilidade Ativa – Metas 40 e 43 - Transporte Público – Meta 48
III	FORTALECER O USO DE **TECNOLOGIA** E DE **INSTRUMENTOS DE GESTÃO** TANTO NO AMBIENTE INTERNO DA CET COMO NOS PROJETOS A SEREM IMPLANTADOS	- Segurança Viária - Meta 39 - Mobilidade Ativa – Metas 41 e 43 - Transporte Público – Meta 48
IV	**OPERAR E FISCALIZAR**, CONTRIBUINDO PARA A PRIORIDADE DA MOBILIDADE ATIVA E DA SEGURANÇA DOS MOTOCICLISTAS	- Segurança Viária - Meta 39 - Mobilidade Ativa – Metas 41 e 43 - Transporte Público – Meta 48
V	GARANTIR **COMUNICAÇÃO** COM A POPULAÇÃO E **CAPACITAÇÃO INTERNA** DURANTE A ELABORAÇÃO E IMPLANTAÇÃO DOS PROJETOS.	- Segurança Viária - Meta 39 - Mobilidade Ativa – Metas 41 e 43 - Transporte Público – Meta 48

2.2 Dentre os esforços necessários no campo da tecnologia, há que ressaltar aqueles que dizem respeito ao tema Governa Corporativa. O tema Governança figurou como um dos 3 pilares do planejamento estratégico dos anos de 2018 a 2021 dessa companhia, e teve por objetivo estabelecer iniciativas que visam aprimorar os aplicativos e tecnologias administrativas, promover a melhoria dos recursos humanos, bem como melhorar os recursos administrativos e de infraestrutura. Os objetivos voltados é de caráter contínuo e possui relação direta com os objetivos

2.3 No contexto global, não há como falarmos sobre investimentos voltados ao fortalecimento do uso da tecnologia, sem discutirmos seus impactos no que se refere aos temas Segurança da Informação e ao Compliance.

2.4 Isto porque, é sabido que a CET possui inúmeras aplicações e plataformas que salvaguardam dados sensíveis, dados e sistemas que podem ser impactados direta e indiretamente pelo crescente aumento no número de invasões e ataques cibernéticos.

2.5 Esse contexto é potencializado ao fato de a Companhia de Engenharia de Tráfego – CET – agora ser responsável por todas as atividades do Departamento do Sistema Viário – DSV, **de acordo com o Decreto 60.982, de 30 de dezembro de 2021**.

2.6 Esse marco aumenta exponencialmente o volume de dados e informações transacionadas pelos agentes, inclusive em relação ao uso do **DSV DIGITAL**, uma ferramenta desenvolvida para viabilizar o atendimento mais ágil e simples aos proprietários de veículos.

2.7 Nesse sentido, há que se considerar, em um primeiro momento, a necessidade de adequação do ambiente tecnológico dessa Companhia ao dispositivo legal, que disciplina o tema segurança da informação, qual seja, a Lei Geral de Proteção de Dados (LGPD). Sobre o tema, é sabido que após os marcos da referida lei, os agentes de tratamento de dados ficam sujeitos às sanções administrativas a serem aplicadas pela autoridade nacional, podendo incorrer em multas, advertências, bloqueio, publicização do ato de sanção, incluindo a paralização/suspensão dos serviços prestados.

2.8 De igual modo, é sabido que nos últimos anos inúmeras bases de dados de empresas ao redor do mundo foram sujeitas a incidentes de segurança, nesse cenário, em um mundo crescentemente digitalizado, a preocupação com a Privacidade e com os dados pessoais não pode ser ignorada.

2.9 As regras de Privacidade de organizações, sejam elas públicas ou privadas, são criadas em conexão com a própria Governança corporativa, irradiando orgânica e construtivamente nas atividades de tratamento de dados, nesse sentido a LGPD compõe 11 pilares e cada um deles visa atender a uma necessidade prevista. Em relação à Segurança, temos um pilar que tangencia o tratamento dos dados forma segura, portanto, a organização deve possuir um programa de segurança da informação que garante a aplicação das medidas de segurança necessárias, alinhadas aos riscos identificados e implementadas desde a concepção de novos produtos, serviços, processos etc.

2.10 Nesse cenário, ao considerarmos o volume de acessos e informações transacionadas pela CET, a disponibilização de novos serviços e a complexidade dos eventos executados pelas áreas internas e externas, bem como o crescente aumento de novas ameaças cibernéticas, tentativas de invasão aos sistemas e ataques, é possível concluir que, sem um processo e/ou ferramenta que possibilite a correta proteção do dado, seja onde ele estiver, a CET estará sujeita a passar por incidentes de segurança com grave impacto ao desempenho institucional, tais como indisponibilidade nos serviços fornecidos, acesso e distribuição ilegal de informações, dados pessoais, dados pessoais sensíveis e tempo investido pela equipe no tratamento e resposta de ocorrências.

2.11 Por fim, por meio da solução de tecnologia que se pretende contratar, buscase, sobretudo, melhorar os avanços voltados para Segurança da informação e dados pessoais frente aos mais diversos desafios, explorando as vantagens oriundas da utilização de Inteligência Artificial e demais solução disruptivas de TIC disponíveis nesse segmento de mercado.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. Levando-se em consideração a atual situação da estrutura de segurança da Companhia de Engenharia de Tráfego-CET, foram especificadas as características de contratação de soluções (hardware e software) e serviços de segurança digital integrados em plataforma única para proteção do ambiente computacional e seus ativos. A plataforma deverá contemplar disponibilidade e capacidade de gestão, garantindo desempenho e proteção dos acessos aos dados e informações sensíveis dos sistemas e informações em custódia, hospedados e processados no ambiente da CET. A Plataforma deverá contemplar os seguintes itens:

3.1.1. Solução de gestão centralizada de chaves criptográficas e criptografia;

3.1.2. Solução de Mapeamento e Classificação de Dados;

3.1.3. Solução de Gestão de Identidade e Acesso;

3.1.4. Solução de Prevenção de Vazamento de dados;

3.1.5. Solução de Gestão de senhas de alto privilégio;

3.1.6. Solução de painel central de gerenciamento de indicadores de segurança;

3.1.7. Serviços de Instalação e Configuração;

3.1.8. Serviços de Treinamento;

3.1.9. Serviços de Operação Assistida.

3.2. Tabela de Composição de Itens

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	Console de Gerenciamento de Chaves Criptográficas	Licença Perpétua / Aquisição	02
2	Criptografia para Sistemas de Arquivos de Servidores	Licença Perpétua / Aquisição	11
3	Criptografia de Registros em Bancos de Dados via Aplicações Web	Licença Perpétua / Aquisição	05
4	Criptografia para Compartilhamento Seguro de Base de Dados	Licença Perpétua / Aquisição	01
5	Módulo de Mapeamento de Classificação de dados.	Licença Subscrição (Mensalidade)	24
6	Solução de gestão de identidade e acesso.	Licença Subscrição (Mensalidade)	24
7	Solução de Prevenção de vazamento de dados.	Licença Subscrição (Mensalidade)	24
8	Solução de gestão de credenciais de alto privilégio	Licença Perpétua / Aquisição	01
9	Painel Central de Gerenciamento de Indicadores de Segurança	Licença Subscrição (Mensalidade)	24
10	Manutenção e Garantia de Console de Gerenciamento de Chaves Criptográficas	Serviço mensal	24
11	Manutenção e Garantia para Criptografia para Sistema de Arquivos de Servidores	Serviço mensal	24
12	Manutenção e Garantia para Criptografia de Registros em Bancos de Dados via Aplicações Web	Serviço mensal	24
13	Manutenção e Garantia para Criptografia de Compartilhamento Seguro de Base de Dados	Serviço mensal	24
14	Manutenção e Garantia para Solução de gestão de credenciais de alto privilégio	Serviço mensal	24
15	Instalação e Configuração de plataforma de criptografia	Serviço	01
16	Treinamento	Serviço	01
17	Serviço de Operação Assistida	Serviço mensal	23

3.3. Vigência

3.3.1. O contrato terá vigência de 24 (vinte e quatro) meses, a contar da data de assinatura do Contrato ou da última dada da assinatura eletrônica registrada no Contrato. Podendo ser renovada até seu limite legal.

3.3.2. Durante o período de vigência das manutenções, estarão inclusas todas as atualizações necessárias para o perfeito funcionamento da solução.

4. DA INDISSOCIABILIDADE DO OBJETO

Visando a mitigação de pontos de falha, decidiu-se, após criteriosos estudos de mercado, que a contratação pela modalidade de serviços gerenciados através de único fornecedor de todos os módulos, irá resguardar os interesses da Companhia de Engenharia de Tráfego - CET, de forma a não tornar o ambiente de segurança da informação, por si só, não gerenciável dentre a heterogeneidade de tecnologias e fornecedores existentes no mercado.

Notadamente, a contratação de fornecedores diferentes para cada módulo, ou subconjunto de módulos, oferecerá riscos no tocante à integração e operação entre eles de forma que as entregas esperadas poderão ser comprometidas, trazendo riscos diretos e indiretos.

Executando a contratação por meio de fornecedores diferentes, certamente haverá durante a execução dos serviços questões técnicas onde cada fornecedor do seu referido módulo poderá se eximir de responsabilidade onerando os demais fornecedores.

Ademais, a contratação de módulos individuais poderá acarretar maior tempo de instalação, aumento de nível de complexidade e consequentemente maior investimento por parte da Companhia de Engenharia de Tráfego - CET.

Cabe ressaltar o comprometimento por parte deste órgão em priorizar qualidade e excelência também no segmento de segurança, buscando conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 - Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

A Companhia de Engenharia de Tráfego - CET, busca fornecedores capazes de prover a solução integrada e coesa, e assim, garantir a melhor entrega dos resultados esperados.

As melhores práticas de segurança atuais versam que as soluções devem possuir interoperabilidade e correlação para que se possa obter o melhor resultado de prevenção, proteção e mitigação de incidentes de segurança.

No tocante as melhores práticas de segurança, coube-nos avaliar ainda as necessidades inerentes ao corpo técnico dos Fornecedores e sua qualificação para implementação, operação e suporte dos serviços, salientando que para correta execução do objeto será imprescindível a existência de profissionais certificados nas áreas de expertise do objeto contratado.

Dessa forma, a Companhia de Engenharia de Tráfego - CET, também balizará as ofertas através de empresas com profissionais que detém comprovadamente o conhecimento e aptidões necessários para a execução e entrega dos serviços demandados.

5. REQUISITOS TÉCNICOS E FUNCIONAIS:

5.1. Gerenciamento de Chaves Criptográficas e Criptografia

5.1.1. A solução deve oferecer recursos para proteger e criptografar os bancos de dados, arquivos e contêineres, além de poder proteger ativos que residem em nuvem, servidores virtuais, big data e servidores físicos;

5.1.2. A solução deverá prover uma console de gerenciamento composta por um conjunto integrado de produtos baseados em uma infraestrutura comum e extensível, com gerenciamento centralizado de políticas e de chaves;

5.1.3. A solução deverá prover uma console única que permita o gerenciamento centralizado de todos os softwares de criptografia, suas chaves criptográficas, políticas de configuração, publicação e controle de acesso dos dados a serem protegidos;

5.1.4. A console deverá possuir controles válidos pelos padrões FIPS 140-2, Common Criteria, para garantir total segurança das chaves criptográficas;

5.1.5. A console de gerenciamento centralizado deverá suportar softwares para as funcionalidades que seguem:

5.1.5.1. Criptografia transparente – para criptografar, controlar o acesso ao dado e oferecer registros de auditoria de acesso aos dados sem impactar nas aplicações, base de dados ou infraestrutura onde quer que os servidores estejam instalados;

5.1.5.2. Integração com SIEM – suportar integração com os sistemas de gerenciamento de logs do mercado;

5.1.5.3. Segurança de container - oferecer criptografia de dados, controle de acesso e registro de acesso ao dado;

5.1.5.4. Segurança de big data - criar isolamento em seus data lakes, mascarar dados confidenciais e controlar a segurança e a conformidade de usuários e administradores;

5.1.5.5. Tokenização e mascaramento de dados - reduzir os custos e o esforço necessários para cumprir com as políticas de segurança e normas regulatórias como o LGPD, GDPR entre outras;

5.1.5.6. Criptografia para aplicações – simplificar o processo de adição de criptografia em aplicações, por meio de APIs (ou outra tecnologia) baseadas em padrões que potencializem operações criptográficas e de gerenciamento de chaves de alto desempenho;

5.1.6. O console deverá ser configurada em alta disponibilidade (HA) com um nó primário e um nó secundário evitando a indisponibilidade do gerenciamento em caso de falha;

5.1.7. Deverá apoiar a incorporação de vários consoles adicionais para fins de configuração de esquemas de tolerância a falhas multinível;

5.1.8. Os softwares instalados nos servidores deverão operar de forma autônoma não causando impacto em caso de perda de comunicação com a console de gerenciamento;

5.1.9. Os softwares deverão realizar a troca/mudança de chaves sem indisponibilidade nos servidores e aplicações;

5.1.10. Cada console deverá ter a escalabilidade para suportar o crescimento;

5.1.11. Detalhes da chave de criptografia não deverão ser divulgados para usuários do sistema para que o algoritmo de criptografia esteja protegido dos usuários da plataforma. Estes deverão ser armazenado de forma segura em um dispositivo dedicado aos serviços de segurança dentro do console;

5.1.12. Serão aceitas soluções de fabricantes distintos, desde que estes fabricantes comprovem interoperabilidade e suporte a solução ofertada;

5.1.13. A console deverá possuir capacidade de gerenciar chaves criptográficas padrão KMIP (Key Management Interoperability Protocol);

5.1.14. Deverá ser compatível com APIs PKCS (Public Key Cryptography Standards) # 11, JCE (Java Cryptography Extension), Microsoft CNG (Criptography API Next Generation) e Microsoft Key Extensible Management;

5.1.15. Deverá ser capaz de oferecer suporte a certificados digitais (X. 509) PKCS # 7, PKCS # 8 e PKCS # 12, chaves de criptografia simétrica: algoritmos 3DES, AES (128, 192, 256), ARIA (128, 192, 256) e assimétrica :algoritmos RSA (1024,2048,4096) e Elliptic Curve;

5.1.16. Deverá ser escalável para oferecer suporte a gerenciamento de software de vários serviços em uma estrutura de multi-tenant e com suporte a configuração de segurança de vários domínios. Para isso, deverá possibilitar configurar diferentes chaves criptográficas de acordo com cada área de operação, se necessário;

5.1.17. A console deverá possibilitar gerenciamento via interface Web além de comandos (CLI) e API (REST);

5.1.18. Deverá requerer autenticação de usuário e senha com integração LDAP e Microsoft Active Directory e, opcionalmente, dois fatores RSA;

5.1.19. Deverá ser capaz de configurar cópias de backup de suas configurações automaticamente ou manualmente;

5.1.20. Requerimentos complementares:

5.1.20.1. Deverá suportar usuários múltiplos;

5.1.20.2. Deverá possuir suporte comprovado para até 1 milhão de chaves criptográficas;

5.1.20.3. Deverá possibilitar cluster para alta disponibilidade (HA);

5.1.20.4. Deverá possuir toolkit e interface de programação;

5.1.20.5. Deverá suportar Integração com infraestrutura de autenticação existente, com fácil configuração;

5.1.20.6. Deverá possuir API RESTful;

5.1.21. Opções de instalação:

5.1.21.1. Sistema virtual com padrões e requisitos da certificação FIPS 140-2 Nível 2, ou certificação compatível;

5.1.21.1.1. O sistema virtual deve ser compatível com VMware, Hyper-V, KVM, AWS e Azure;

5.1.21.2. Sistema de hardware com padrões e requisitos de certificação FIPS 140-2 Nível 2, ou compatível;

5.2. Criptografia para Sistemas de Arquivos de Servidores

5.2.1. Deverá oferecer controle de acesso de usuários, incluindo usuários privilegiados, e registro detalhado de auditoria de acesso visando atender aos requisitos de conformidade e práticas recomendadas para proteção de dados;

5.2.2. Deverá prover criptografia de servidor de arquivo (dado não estruturado) para dados em repouso com gerenciamento centralizado de chaves;

5.2.3. Deverá fornecer criptografia para a estrutura de pastas e arquivos dos SGBD's (Sistemas Gerenciadores de Banco de Dados) para dados em repouso com gerenciamento centralizado de chaves;

5.2.4. O processo de criptografia deverá ser executado por softwares que serão instalados nos servidores de banco de dados;

5.2.5. O software ou equivalente deverá residir no sistema operacional ou na camada de dispositivo, e a criptografia e a descriptografia deverão ser transparentes para todos os aplicativos executados acima dela;

5.2.6. Deverá ser compatível com servidores físicos e versões virtualizadas;

5.2.7. Sua implementação não deverá exigir qualquer alteração no servidor de arquivo ou processo para manuseio do dado pelo usuário final;

5.2.8. Deverá ser capaz de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações não estruturadas;

5.2.9. A implementação destes não deverão gerar uma carga incremental (processamento, memória e espaço em disco), típica em servidores, de mais de 5%, sendo tolerável picos esporádicos de até 10%;

5.2.10. Além de criptografar a estrutura de pastas e arquivos do banco de dados, aplicações e Servidores de Arquivo, os softwares deverão ser capazes de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações estruturadas e não estruturadas;

5.2.11. Os softwares deverão registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso;

5.2.12. A solução deve operar plenamente sem a necessidade de instalação de softwares nas estações de trabalhos que acessarão os servidores, bem como não solicitar autenticação adicional durante o acesso aos dados criptografados no servidor;

5.2.13. As políticas de controle de acesso deverão ser aplicadas aos usuários privilegiados do sistema e estes não deverão possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio;

5.2.14. Essas diretivas deverão permitir ser baseadas em usuário, processo, tipo de arquivo, dia e horário;

5.2.15. As políticas deverão ser aplicadas aos usuários locais, ou igualmente integradas no AD ou no LDAP;

5.2.16. Os softwares deverão ter a capacidade de armazenar chaves criptográficas em memória para que eles não exijam conectividade com a console de gerenciamento para poder aplicar processos de criptografia e descriptografia;

5.2.17. Os registros (logs) de atividade do usuário deverão ter a capacidade de ser enviado para uma solução de SIEM através de um servidor de syslog ou no formato CEF, em tempo real e nativamente;

5.2.18. A solução deverá suportar ambiente em nuvem, tais como AWS, Azure, Google Cloud, Oracle Cloud e IBM, pelo menos;

5.2.19. Deverá registrar todas as tentativas de acesso de usuários, aplicativos e processos;

5.2.20. Deverá possuir políticas de acesso baseadas em função para identificar qual dado foi acessado, quem o acessou, como o acessou, o local e quando foi acessado;

5.2.21. Deverá permitir que usuários privilegiados executem seu trabalho sem acesso a informações contidas nos arquivos criptografado;

5.2.22. Deverá ser compatível com os sistemas operacionais:

5.2.22.1. Microsoft: Windows Server 2019, 2016 2012 ou superior;

5.2.22.2. UNIX: IBM AIX;

5.2.22.3. Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, and Ubuntu;

5.2.23. Deverá permitir no mínimo criptografia para a estrutura de pastas e arquivos para múltiplos fabricantes de banco de dados, tais como:

5.2.23.1. Oracle (Windows, Linux);

5.2.23.2. DB2 (Windows, Linux);

5.2.23.3. Informix (Windows, Linux);

5.2.23.4. MySQL (Windows, Linux);

5.2.23.5. MS SQL (Windows);

5.2.23.6. Postgree (Linux);

5.2.23.7. MongoDB (Windows e Linux);

5.2.23.8. Sybase (Linux);

5.3. Criptografia de Registros em Bancos de Dados via Aplicações Web

5.3.1. Permitir a Tokenização, independentemente do tipo de banco de dados, com mascaramento dinâmico, para promover a anonimização/pseudonimização de dados, incluindo dados pessoais, seja no Data Center, ambiente de big data ou Nuvem.

5.3.2. Permitir tokenização irreversível (one-time Tokenization) para aplicar o conceito pleno da anonimização (não reversível) conforme LGPD Artigo 12;

5.3.3. Possuir servidores de token escalável;

5.3.4. Comunicação via TLS autenticado mutuamente;

5.3.5. Interface REST API com chamadas individuais e em lote;

5.3.6. Permitir geração de Tokens Aleatórios;

5.3.7. Compatível com FPE FF1, Tokens FF3;

5.3.8. Permitir Mascaramento Dinâmico ou Estático de Dados;

5.3.9. Gerenciamento de chaves e políticas;

5.3.10. Suporte AD / LDAP;

5.3.11. Suporte a dados numéricos e alfanuméricos;

5.3.12. Permitir a criação de tokens em formatos numéricos, de texto e de data para aplicativos únicos ou múltiplos;

5.3.13. Permitir utilizar grupos de usuários LDAP para decidir quais informações são exibidos para grupos específicos;

5.3.14. Suportar servidor de tokens no formato virtual de acordo com a escolha da CET: OVF, ISO, VHD, Microsoft Azure Marketplace ou Amazon AMI;

5.3.15. Restringir o acesso a ativos confidenciais sem alterar os esquemas do banco de dados, sem interrupções;

5.3.16. Proteger dados em trânsito e em repouso;

5.3.17. Mascarar os dados em ambiente de desenvolvimento, teste e terceirizados com acesso ao banco de dados;

5.3.18. Proteger usuários DBAs, administradores de sistema, root, com acesso direto ao banco de dados, contra ação de usuários mal-intencionados;

5.4. Criptografia para Compartilhamento Seguro de Bases de Dados

5.4.1. Este software deverá permitir o mascaramento dos dados sensíveis para permitir o compartilhamento seguro com terceiros, ambientes de teste, ambientes de desenvolvimento e outros casos de uso aplicáveis;

5.4.2. O funcionamento deverá ser baseado em tabela e/ou coluna;

5.4.3. A solução deverá ser customizável e de alta performance;

5.4.4. A solução deverá suportar, pelo menos, as operações de criptografia / Tokenização e descriptografia / detokenização de tabelas e / ou colunas;

5.4.5. A solução deverá ser "transparente" para a aplicação ou banco de dados com acesso via conexão JDBC, sem a necessidade de requerer alterações ou instalações adicionais no servidor de banco de dados;

5.4.6. A solução deverá suportar, pelo menos, arquivo CSV, Oracle, Microsoft SQL Server, MySQL, Postgree, MongoDB e DB2;

5.4.7. A solução deverá permitir replicação de arquivo para arquivo, banco de dados para banco de dados, arquivo para banco de dados e banco de dados para arquivo;

5.4.8. Pelo menos os seguintes modelos deverão ser suportados: Standard AES Encryption, Batch random Tokenization e Batch FPE FF3/FF1

5.5. Identificação e Classificação de Dados

5.5.1. A solução deverá possibilitar a descoberta de dados, em ambiente de dados estruturados e não estruturados, armazenados em diferentes repositórios, tais como:

5.5.1.1. Servidores de Arquivos;

5.5.1.2. Banco de Dados;

5.5.1.3. Big data;

5.5.1.4. Estações de trabalho;

5.5.2. A solução deve permitir, através de interface única, realizar o levantamento e entendimento dos dados existentes, sua localização e riscos associados, permitindo:

5.5.3. Atender aos requisitos de privacidade;

5.5.4. Obter visibilidade sobre os dados que estão em risco de exposição;

5.5.5. Suportar a criação de plano de privacidade e proteção de dados;

5.5.6. A solução ofertada deverá possibilitar, pelo menos, quatro níveis de classificação de dados por padrão:

5.5.6.1. Restrito;

5.5.6.2. Privado;

5.5.6.3. Interno;

5.5.6.4. Público;

5.5.7. A solução deve atribuir pontuações de risco que permitam identificar o nível de sensibilidade dos dados, como arquivos e bancos de dados, agregando os seguintes parâmetros:

5.5.7.1. Nível de proteção;

5.5.7.2. Quantidade de elementos encontrados;

5.5.7.3. Localização;

5.5.7.4. Quantidade de dados confidenciais;

5.5.8. As pontuações de risco devem permitir identificar os dados com maior exposição e permitir priorizar medidas de proteção;

5.5.9. A solução deve suportar ambientes:

5.5.9.1. Armazenamento local em Hard Disk e Memória dos computadores;

5.5.10. Armazenamentos em rede:

5.5.10.1. Compartilhamento Windows CIFS e SMB;

5.5.10.2. Unix File System NFS;

5.5.11. Bancos de Dados:

5.5.11.1. IBM DB2;

5.5.11.2. Oracle;

5.5.11.3. SQL;

5.5.11.4. Big Data:

5.5.11.5. Clusters Hadoop

5.5.12. A solução deve suportar os seguintes tipos de arquivos:

5.5.12.1. Banco de Dados;

5.5.12.2. Access;

5.5.12.3. Dbase;

5.5.12.4. SQLite;

5.5.12.5. MSSQL MDF & LDF;

5.5.12.6. MySQL

5.5.13. Arquivos de Imagens:

5.5.13.1. BMP;

5.5.13.2. FAX;

5.5.13.3. GIF;

5.5.13.4. JPG;

5.5.13.5. PDF;

5.5.13.6. PNG;

5.5.13.7. TIF;

5.5.14. Arquivos Compactados:

5.5.14.1. bzip2;

5.5.14.2. Gzip (todos os tipos);

5.5.14.3. TAR;

5.5.14.4. Zip (todos os tipos);

5.5.15. Microsoft Backup:

5.5.15.1. Microsoft Binary / BKF;

5.5.16. Microsoft Office:

5.5.16.1. v5;

5.5.16.2. v6;

5.5.16.3. 95;

5.5.16.4. 97;

5.5.16.5. 2000;

5.5.16.6. XP;

5.5.16.7. 2003 e superiores;

5.5.17. Open Source:

5.5.17.1. Star Office;

5.5.17.2. Open Office;

5.5.17.3. BR Office

5.5.17.4. Libre Office

5.5.18. Padrões abertos:

5.5.18.1. PDF;

5.5.18.2. HTML;

5.5.18.3. CSV;

5.5.18.4. TXT;

5.5.19. A solução deve classificar os dados como:

5.5.19.1. Dado pessoal;

5.5.19.2. Dados financeiros, com base em modelos integrados ou técnicas de classificação;

5.5.20. Deve possibilitar a identificação de informações padronizadas do Brasil, tais como:

5.5.20.1. Registro Geral (RG);

5.5.20.2. Cadastro de Pessoa Física (CPF);

5.5.20.3. Carteira Nacional de Habilitação (CNH);

5.5.20.4. Passaporte;

5.5.21. A solução deve permitir a inclusão de modelos de políticas (descoberta e classificação) específicas para LGPD;

5.5.22. A solução deve fornecer relatórios detalhados para demonstrar conformidade com a Lei Geral de Proteção de Dados (LGPD);

5.5.23. A solução deve possibilitar a classificação de dados utilizando:

5.5.23.1. Expressões Regulares (Regex);

5.5.23.2. Padrões (Patterns);

5.5.23.3. Algoritmos;

5.5.23.4. Contexto;

5.5.24. A solução deve possibilitar ser implementada “com” ou “sem” softwares instalados;

5.5.25. A solução deve oferecer as seguintes características funcionais:

5.5.25.1. Definir as políticas de privacidade de dados, locais e perfis de varredura e de classificação;

5.5.25.2. Localizar dados estruturados e não estruturados, através de toda a organização em ambientes big data, banco de dados e sistema de armazenamento de arquivos;

5.5.25.3. Classificar dados pessoais e sensíveis, baseado em modelos pré-configurados e técnicas de classificação;

5.5.25.4. Entender a natureza do dado e seus riscos, oferecendo visualizações;

5.5.25.5. Gráficos e relatórios de análise de risco, status e alertas durante todo o ciclo de vida do dado.

5.5.26. A solução deverá ser dimensionada para executar varreduras em volumes de 50TB (Cinquenta TeraBytes);

5.6. Solução de Gestão de Identidade e Acesso

5.6.1. A solução deverá ser dimensionada para 2000 (dois mil) usuários;

5.6.2. Garantir 99.999% de disponibilidade para acesso remoto;

5.6.3. Garantir visibilidade e gerenciamento de todos os serviços e usuários do MFA;

5.6.4. A solução de MFA deve suportar diversos fatores de autenticação, tais como:

5.6.4.1. Soft Token;

5.6.4.2. Hard Token

5.6.4.3. Mobile App;

5.6.4.4. SMS;

5.6.4.5. SmartCard;

5.6.4.6. PIV;

5.6.4.7. FIDO;

5.6.4.8. Certificados Digitais;

5.6.4.9. Push;

5.6.5. Deve conter políticas granulares para esses tokens, de acordo com a necessidade e adequação de cada negócio;

5.6.6. Deve suportar mais de um tipo de token para o usuário;

5.6.7. A Solução de MFA de suportar diversos sistemas operacionais e identificar dentro da ferramenta:

5.6.7.1. Windows 7/8/10/11;

5.6.7.2. MAC OS;

5.6.7.3. LINUX.

5.6.8. A Solução deve também suportar dispositivos móveis:

5.6.8.1. Android (Diversas versões);

5.6.8.2. IOS;

5.6.9. A Solução deve ser capaz de identificar o dispositivo pelo sistema operacional e criar políticas de acordo com a necessidade do negócio baseada em cada SO, incluso sistemas operacionais de dispositivos móveis;

5.6.10. A Solução deverá suportar Auto registro. Uma página na qual o próprio usuário poderá solicitar um token, avisar que perdeu, solicitar um outro tipo de token, caso tenha esquecido ou perdido o token original;

5.6.11. A solução deverá suportar Geolocalização, e criar políticas de acordo com esse perfil;

5.6.12. Gerenciar do Risco através de políticas de contexto, tais como tipo de rede, tipo de sistema operacional, tipo de dispositivo e geolocalização;

5.6.13. A solução deverá verificar o tipo de conexão, anonimizada ou não e ser possível criar perfis de acordo;

5.6.14. A solução deve suportar integração com LDAP e AD;

5.6.15. A solução de prover relatórios de auditoria e poder exportar os dados;

5.6.16. Deve suportar integração com SIEM;

5.6.17. A solução deve ser capaz de criar políticas de acordo com cada perfil, grupo de usuários;

5.6.18. A solução deve ser capaz de criar políticas de acordo com cada aplicação;

5.6.19. A solução deve ter a opção de verificar se já é um dispositivo conhecido;

5.6.20. A solução deverá permitir Single Sign on;

5.6.21. Mesmo com o Single Sign on, deverá ser possível criar políticas de verificação em cada aplicação;

5.6.22. A Solução deve conter um dashboard informando os acessos por aplicação (Acessos validos e negados);

5.6.23. A solução deve conter um dashboard informando os acessos por políticas (Acessos Validos e negados);

5.6.24. A solução deve prover informações a respeito de qual IP está sendo feita a autenticação, e qual método utilizado para o duplo fator de autenticação;

5.6.25. A Solução deve prover para o usuário final, um portal, consolidando todas a aplicações nas quais ele tem acesso;

5.6.26. Suportar integrações via Radius;

5.6.27. Suportar integrações via SAML 2.0;

5.6.28. A solução deverá suportar as 27 (vinte e sete) bases de usuários de aplicações legadas, que se utilizam de sistemas de autenticação diferentes, sejam elas:

5.6.28.1. SQL;
5.6.28.2. LDAP

5.6.28.3. AD

5.6.28.4. ODBC

5.6.28.5. Lotus

5.6.28.6. Novell

5.6.28.7. Outros via mapeamento de campos

5.6.29. A solução deverá se adequar às aplicações legadas, utilizando-se de meios próprios, mesmo que isso incorra no desenvolvimento e adaptação;

5.6.30. A solução deverá suportar meios para integração com as aplicações legadas, fornecendo um conjunto de bibliotecas (API e SDK);

5.6.31. A solução deve oferecer integração com as aplicações legadas minimamente com as funcionalidades de duplo fator de autenticação (MF2) e rastreabilidade (data e hora de entrada e saída);

5.7. Solução de Prevenção de Vazamento de Dados

5.7.1. A solução deverá ser dimensionada para 2000 (dois mil) usuários;

5.7.2. Deverá ser capaz de detectar e identificar dados acessados pelo usuário em trânsito ou dentro da rede e ser armazenado localmente ou em um compartilhamento de rede;

5.7.3. Deverá ser gerenciada por uma console separadamente das estações de trabalho;

5.7.4. Deverá fornecer ações capazes de relatar um incidente, bloquear o acesso do usuário aos dados e colocar e-mails em quarentena que contenham dados confidenciais;

5.7.5. Deverá, por meio de agentes instalados, permitir o controle dos dados em uso, como ações do usuário relacionadas à cópia de informações, impressão de arquivos classificados e captura de tela (Print Screen);

5.7.6. O agente deverá utilizar regras para proteger dados confidenciais contra vazamento nos seguintes vetores:

5.7.6.1. Software de clipboarding (copiar e colar);

5.7.6.2. Aplicações em nuvem;

5.7.6.3. E-mail;

5.7.6.4. Compartilhamento de rede;

5.7.6.5. Impressão;

5.7.6.6. Captura de tela;

5.7.6.7. Aplicativos e navegadores específicos;

5.7.6.8. Postagens na Web;

5.7.7. Deverá ser capaz de restringir as regras de proteção de dados a grupos de usuários do serviço de diretórios;

5.7.8. Deverá ser capaz de restringir as regras de proteção de dados a grupos de máquinas ou equipamentos que fazem parte da mesma faixa de endereços IP com agentes instalados;

5.7.9. Deverá ser capaz de restringir as regras de proteção de dados com base no funcionamento do sistema operacional, minimamente:

5.7.9.1. Windows 7 e superior,

5.7.9.2. Windows Server 2008 R2 e superior;

5.7.10. Deverá ser capaz de replicar conteúdo sensível que tenha violado uma regra de proteção de dados em sua totalidade;

5.7.11. Deverá permitir a execução de políticas independentemente da conexão do usuário;

5.7.12. Deverá utilizar técnicas e dicionários de reconhecimento de padrões de texto predefinidos;

5.7.13. As políticas deverão abranger Classificação, Rastreamento, Monitoramento e Proteção;

5.7.14. Deverá permitir a configuração de classificações da informação, pelo menos:

5.7.14.1. Confidencial, Restrita e Pública;

5.7.15. Deverá permitir para cada classificação, que as informações a serem protegidas possam ser definidas. Os métodos de definição devem incluir:

5.7.15.1. Padrões Avançados (Exemplo: Regex);

5.7.15.2. Dicionários;

5.7.15.3. Arquivos TrueType;

5.7.15.4. Origem ou Destino;

5.7.15.5. Grupos de aplicativos;

5.7.16. Deverá permitir que grupos de aplicação sejam adicionados à solução como critério de classificação de dados;

5.7.17. Deverá possuir método de identificação e rastreamento de conteúdo;

5.7.18. Deverá permitir que classificações sejam baseadas em pelo menos as seguintes informações de contexto do arquivo:

5.7.18.1. Aplicação web da qual o arquivo se originou;

5.7.18.2. Compartilhamento de rede da qual foi copiada;

5.7.18.3. Arquivos baixados de serviços de nuvem;

5.7.19. Deverá ser capaz de varrer todos os arquivos armazenados em um determinado repositório para proteger conteúdo classificado;

5.7.20. Deverá permitir a classificação manual dos arquivos, adicionando etiquetas (Tags) e permitindo seu rastreamento;

5.7.21. Deverá ter a capacidade de criar regras para identificar conteúdo sensível e tomar uma ação específica;

5.7.22. Deverá permitir a criação de regras para controlar a distribuição não autorizada de dados classificados;

5.7.23. Deverá conter mecanismos de proteção que impeçam a desinstalação do agente localmente;

5.7.24. Deverá permitir que o agente seja executado no modo de segurança no sistema operacional Windows;

5.7.25. Deverá ter classificações definidas por padrão, por exemplo: EAR, HIPAA,PCI, PHI, SOX etc.

5.7.26. Deverá ter a capacidade de identificar informações confidenciais com base em padrões avançados (expressão regular);

5.7.27. Deverá permitir o uso de propriedades de documentos do Microsoft Office para classificá-lo;

5.7.28. Deverá permitir a definição de classificação com base na origem ou destino, suportando pelo menos:

5.7.28.1. Aplicação;

5.7.28.2. Grupo de Usuários;

5.7.28.3. Compartilhamento de rede;

5.7.28.4. Deverá possuir modelos definidos por fabricante;

5.7.29. Deverá, além dos modelos já incluídos na solução, criar livremente padrões e dicionários avançados para identificar informações confidenciais nas estações de trabalho;

5.7.30. Deverá permitir a inclusão de documentos que não devem ser detectados pela solução (Whitelist);

5.7.31. Deverá ser capaz de procurar informações confidenciais armazenadas localmente e na nuvem;

5.7.32. Deverá identificar o local onde os dados confidenciais são armazenados;

5.7.33. Deverá permitir a visualização de todos os dados indicados na varredura através da console intuitivo;

5.7.34. Deverá suportar classificação de conteúdo, tais como:

5.7.34.1. Cloud Store;

5.7.34.2. Documentos do Microsoft Office;

5.7.34.3. Arquivos da Adobe;

5.7.34.4. Arquivos compactados;

5.7.35. Deverá permitir o agendamento de tarefas periódicas para a varredura do repositório;

5.7.36. Deverá permitir que o administrador configure varreduras distintas;

5.7.37. A varredura de inventário deverá fornecer uma visão geral dos tipos de arquivos em cada repositório, executando apenas:

5.7.37.1. Coleta de metadados;

5.7.37.2. Classificação dos metadados em diferentes tipos de conteúdo e análise de atributos, como tamanho do arquivo, localização de armazenamento e extensão;

5.7.38. A varredura de classificação deverá permitir entender quais tipos de dados existem em repositórios;

5.7.39. Deverá comparar o conteúdo analisado com classificações estabelecidas, por exemplo, padrões de texto ou dicionários;

5.7.40. A varredura de remediação deverá permitir encontrar dados que violem uma determinada política de sensibilidade de dados estabelecida;

5.7.41. Deverá ter a capacidade de realizar a descoberta em agentes distribuídos em estações de trabalho, permitindo a descoberta de conteúdo em:

5.7.42. Sistema de arquivos local em estações de trabalho com sistema operacional Windows;

5.7.43. Servidor de arquivos;

5.7.44. A solução através do agente deverá permitir que a detecção de um arquivo sensível seja automaticamente classificada pela solução;

5.8. Solução de Gestão de Senhas de Alto Privilégio

5.8.1. Será utilizada para armazenamento seguro e controle de credenciais não pessoais e privilegiadas em Servidores Linux/Unix, Windows, Sistemas, Aplicações Web, Bancos de Dados, Estações de Trabalho e Dispositivos de Rede;

5.8.2. Deverá prover autenticação transparente no sistema-alvo ou dispositivo de rede. A solução deverá iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um proxy para a sessão entre o usuário e o sistema-alvo, de forma que a senha não seja exposta ao solicitante do acesso;

5.8.3. Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências;

5.8.4. Deverá ser baseada em appliance físico ou virtual com banco de dados proprietário e embarcado, a fim de garantir maior segurança e melhor desempenho da solução;

5.8.5. Possibilitar gerenciamento e utilização da solução através de interface Web;

5.8.6. Deverá ser compatível com os principais navegadores de mercado;

5.8.7. Deverá permitir segregação de funções, baseado em perfis de acesso;

5.8.8. Permitir login dos usuários da solução utilizando dois fatores de autenticação;

5.8.9. Permitir que dois ou mais usuários solicitarem acesso a mesma conta privilegiada e/ou genérica, sem comprometimento da rastreabilidade;

5.8.10. Permitir aos administradores se autenticarem na interface de gerência da solução através de certificado digital;

5.8.11. A interface Web deverá suportar a utilização de certificados digitais válidos pela ICP-Brasil e certificados auto assinados gerados pela própria solução;

5.8.12. Ser capaz de operar como proxy de conexões via SSH/TELNET para qualquer dispositivo gerenciado, sem a necessidade de abertura de um Terminal Service;

5.8.13. A solução deverá prover conexões RDP controladas;

5.8.14. Autenticar de forma confiável todas as requisições de senhas realizadas pela solução, com a finalidade de impedir que qualquer usuário ou código malicioso tenha acesso ao repositório de senhas;

5.8.15. Toda a transmissão de dados entre os componentes da solução deverá ser criptografada;

5.8.16. Sobre a utilização de padrões criptográficos por determinadas funcionalidades, a solução deverá atender aos seguintes requisitos:

5.8.16.1. Utilizar algoritmo AES-256 para criptografia do tráfego de informações;

5.8.16.2. Para operações de autenticação e de acordo de chave de sessão, deve permitir a utilização de algoritmos dos sistemas de criptografia de chave pública RSA, Google Autenticator ou ECC;

5.8.16.3. Para os algoritmos do sistema de criptografia RSA, deve permitir a utilização de chaves;

5.8.17. A solução deverá ser compatível com os seguintes sistemas/aplicações:

5.8.17.1. Sistemas Operacionais: Windows Server 2008 e superiores, Red Hat Enterprise Linux (diferentes builds) e MAC OS;

5.8.17.2. Aplicações Windows: Contas de serviço englobando contas de serviço do SQL server em cluster, tarefas agendadas, pools de conexão do IIS, COM+, usuário anônimo do IIS, serviços de Cluster;

5.8.17.3. Sistemas Gerenciadores de Banco de Dados: Oracle, MSSQL, MySQL, Postgree;

5.8.17.4. Appliances de Segurança: CheckPoint, Fortinet, Cisco, IBM, SourceFire e Imperva;

5.8.17.5. Dispositivos de redes: Cisco, D-Link, HP, 3com, Alcatel, Foundry, Brocade e ARUBA;

5.8.17.6. Aplicações: WebLogic, JBOSS, Tomcat, Peoplesoft, Oracle Application Server, Apache e IIS;

5.8.17.7. Serviços de Diretórios: Active Directory (AD) e OpenLDAP;

5.8.17.8. Possuir integração nativa com soluções de SIEM/Syslog;

5.8.17.9. Possuir workflow de aprovação para uso de credenciais;

5.8.17.10. Oferecer armazenamento e consulta de logs que forneçam ao menos, as seguintes informações:

5.8.17.11. Identificação do usuário que realizou determinado acesso a um dispositivo;

5.8.17.12. Identificação de quem aprovou o acesso do usuário;

5.8.17.13. Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto;

5.8.18. Deverá prover, ao menos, os seguintes filtros para a recuperação de logs:

5.8.18.1. Usuário;

5.8.18.2. Sistema-alvo acessado

5.8.18.3. Tipo de atividade

5.8.18.4. Intervalo de tempo (data/hora/minuto inicial e final)

5.8.19. A solução deverá vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades da solução;

5.8.20. Deverá disponibilizar os Templates de troca de senha de forma que possam ser abertos, editáveis e auditáveis;

5.8.21. A solução deverá não deverá depender de sistema operacional externo e/ou banco de dados que gerem a necessidade de licenças adicionais de outros fabricantes.

5.8.22. A solução deverá possibilitar a configuração em cluster de contingência, alta disponibilidade (HA) ou recuperação de desastres (DR);

5.8.23. A solução deverá possibilitar a configuração do backup da solução e seus dados conforme Política de Backup.

5.8.24. A solução deverá exibir opções de Gráficos e Dashboards para operação e gestão da ferramenta;

5.8.25. A solução deverá estar aderente às Normas ISO/IEC 27.001.

5.8.26. Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos ou dispositivos de rede;

5.8.27. Possibilitar a geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança;

5.8.28. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;

5.8.29. Oferecer a possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;

5.8.30. Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo;

5.8.31. Executar a liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata;

5.8.32. Deverá provisionar usuários locais em servidores Linux/Unix, Windows ou dispositivos de rede;

5.8.33. A solução deverá notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;

5.8.34. Permitir o monitoramento on-line do uso das contas e desligamento da sessão;

5.8.35. Apresentar recurso para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade;

5.8.36. Deverá oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos;

5.8.37. Oferecer a possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão caso o usuário execute um comando indevido;

5.8.38. A solução deverá buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;

5.8.39. A solução deverá possibilitar a configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;

5.8.40. Oferecer a possibilidade de geração de relatórios baseados nos logs e exportá-los;

5.8.41. A solução deverá possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha para recuperações no caso de falha total da solução;

5.8.42. Deverá utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (Hash), Path e endereço IP do host a serem acessados pela solução;

5.8.43. Oferecer a possibilidade de comunicação com os serviços de diretório via protocolo LDAPS;

5.8.44. Oferecer a possibilidade de implementação SNMP sobre IPv6;

5.8.45. Implementar a especificação IETF RFC 2460, referente ao protocolo IPv6;

5.8.46. Oferecer a possibilidade de implementar a MIB II, conforme RFC 1213;

5.8.47. Suportar sincronização do relógio interno via protocolo NTP e atualização automática do horário de verão com suporte e customização local;

5.8.48. Deverá controlar a elevação de privilégio em estações de trabalho;

5.8.49. Oferecer a possibilidade de mapear compartilhamentos de rede com um usuário administrador, diferente do usuário logado na máquina.

5.8.50. A solução deverá ser dimensionada para:

5.8.50.1. Usuários que se utilizarão da solução para acesso às credenciais de alto privilégio: 9 (nove) usuários;

5.8.50.2. Quantidade de servidores: 24 (vinte e quatro);

5.8.50.3. Quantidade de dispositivos de rede: 200 (duzentos);

5.8.50.4. Servidores de banco de dados: 40 (quarenta);

5.8.50.5. Quantidade de sessões concorrentes: 10 (dez);

5.9. Painel Central de Indicadores de Segurança

5.9.1. Possuir interface web em português-brasileiro para toda operação, sendo compatível no mínimo com os navegadores Edge, Internet Explorer, Firefox, Google Chrome e Safari;

5.9.2. Possibilitar autenticação de usuários através de base própria, servidor LDAP ou equivalente;

5.9.3. Possuir interface responsiva, possibilitando seu acesso através de dispositivos móvel;

5.9.4. Deverá estar disponível para acesso via HTTPS;

5.9.5. Deverá disponibilizar no mínimo três perfis de usuário: Operador, Analista e Administrador (com estas denominações ou equivalentes);

5.9.6. A solução deverá permitir a customização de painéis em função do perfil do usuário e utilização interna (painéis públicos e privados);

5.9.7. A customização dos painéis se dará através da coleta de métricas e indicadores das diversas soluções fornecidas, incluindo as já existentes;

5.9.8. A coleta das métricas e indicadores poderá ser realizada através de API's, scripts ou desenvolvimento de código específico;

5.9.9. A solução deverá oferecer inicialmente e minimamente duas métricas de cada solução.

6. DAS LICENÇAS

6.1. As licenças deverão ser disponibilizadas através de arquivo e/ou chave de licenciamento disponibilizado pelo fabricante nomeados ao cliente final, e com os respectivos números de série.

6.2. Na ocasião da disponibilização das licenças, deverão ainda ser entregues os aplicativos instaladores (executáveis/binários) acompanhados de documentação técnica em formato digital (manuais de operação) de cada software que compõe a solução.

7. PRAZO CONTRATUAL

7.1. O Contrato terá duração de 24 (vinte e quatro) meses, contados da assinatura do Contrato ou da última assinatura digital, podendo ser renovado/prorrogado pelo período legal.

8. SERVIÇO DE SUPORTE TÉCNICO, MANUTENÇÃO E GARANTIA

8.1. Os serviços de suporte técnico e garantia abrangem:

8.1.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

8.1.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente da solução;

8.2. Os serviços de suporte técnico e garantia abrangem todas as soluções fornecidas pela contratada no âmbito dessa contratação.

8.3. Os serviços de suporte técnico e garantia de toda a solução deverão ser prestados por um período de 24 (vinte e quatro) meses e deverão ser iniciados a partir da data Emissão do Termo de Aceite e Entrega da Solução.

8.4. Os serviços de suporte técnico poderão ser prestados de forma remota ou presencial no endereço da **CET**.

8.5. Os bens e produtos adquiridos devem ser licenciados de forma que o suporte e a garantia permitam as atualizações dos sistemas e ferramentas durante a vigência do contrato. Deverão estar incluídas tanto as atualizações de segurança, quanto as atualizações para novas versões dos softwares licenciados, quando disponibilizadas, independente da política de comercialização do fabricante.

8.6. Todas os sistemas ou ferramentas que fazem parte da solução deverão ser disponibilizados na versão mais recente disponibilizada pelo fabricante.

8.7. A **CONTRATADA** deve garantir que todas as personalizações e configurações realizadas sejam automaticamente portadas para novas versões em caso de atualização, reinstalação ou upgrade, dispensando a necessidade de migrações ostensivas e onerosas.

8.8. O serviço Suporte Técnico e Manutenção servirá para que a contratada, através de equipe própria e comprovadamente especializada na solução, execute serviços inerentes às rotinas técnicas operacionais dos softwares fornecidos.

8.9. Os serviços de Suporte Técnico, Manutenção e Garantia serão mensurados como serviço mensal, tendo sua verificação a partir da constante estabilidade e evolução da Solução no ambiente da Companhia de Engenharia de Tráfego - CET, totalmente integrada com os diversos segmentos da rede corporativa.

9. SERVIÇO DE OPERAÇÃO ASSISTIDA

9.1. A operação assistida deverá ser demandada através de ordem de serviço da abertura de chamado;

9.2. Quando demandado, o horário de execução do serviço de operação assistida será baseado no regime 24x7, devendo a contratada estar disponível 24h por dia;

9.3. A Contratada deverá disponibilizar telefone tipo 0800 ou 011 ou aplicação WEB para abertura dos chamados;

9.4. O serviço de operação assistida poderá ser executado remotamente ou, quando solicitado, presencialmente;

9.5. As seguintes atividades técnicas operacionais compõem o serviço de operação assistida:

9.5.1. Correlação básica de logs

9.5.2. Troubleshooting problemas de comunicação com os softwares;

9.5.3. Backup de configurações e chaves;

9.5.4. Atualização de software ou patch;

9.5.5. Análise, validação e aprovação de políticas, quando necessário;

9.5.6. Configuração de novos softwares quando necessário;

9.5.7. Criação, alteração e configuração de novas políticas;

9.5.8. Refinamentos e melhorias no ambiente;

9.5.9. Confecção de relatórios mensais da saúde e principais eventos do gerenciamento;

9.5.10. Monitoramento do ambiente baseados em detecção e notificação de comportamentos suspeitos;

9.5.11. Apoio aos para identificação de causas-raiz de incidentes;

9.5.12. Sanar quaisquer dúvidas para questões da operação da solução;

9.6. O serviço de Operação Assistida será mensurado como serviço mensal, tendo sua verificação a partir da constante estabilidade e evolução da Solução no ambiente da Companhia de Engenharia de Tráfego - CET, totalmente integrada com os diversos segmentos da rede corporativa.

10. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

10.1. A empresa contratada, observando a regra contida no item 12.4 deste Anexo, deverá apresentar o projeto de implantação que norteará a execução dos serviços de ativação das licenças;

10.2. O projeto de instalação e implantação deverá conter minimamente os seguintes detalhamentos:

10.2.1. Objetivo;

10.2.2. Recomendações, premissas e restrições;

10.2.3. Matriz de Relacionamentos e Responsabilidades;

10.2.4. Descrição das funções dos envolvidos no projeto;

10.2.5. Topologias física e lógica;

10.2.6. Plano de endereçamento IPv4, Plano de VLANs, Plano de Roteamento;

10.2.7. Padronização de hostnames, DNS, SNMP e NTP;

10.2.8. Plano de retorno em caso de problemas

10.2.9. Plano de licenciamento do ambiente virtual;

10.2.10. O projeto deverá ser conduzido em fases:

10.2.10.1. INICIAÇÃO

10.2.10.1.1. A CONTRATADA deverá criar a visão do projeto e definirá o escopo de trabalho necessário para trazê-la para a realidade;

10.2.10.2. PLANEJAMENTO

10.2.10.2.1. Deverá consistir na elaboração dos processos a serem utilizados na implantação do projeto e revisão de todas as questões técnicas necessárias à instalação física e lógica da plataforma, incluindo:

10.2.10.2.1.1. Espaço físico em gabinetes (racks);

10.2.10.2.1.2. Energia elétrica conforme especificação dos fabricantes;

10.2.10.2.1.3. Cabeamento de dados em cobre ou fibra ótica conforme o caso;

10.2.10.2.1.4. Padrões de nomenclatura;

10.2.10.2.1.5. Lista de contatos das equipes de tecnologia;

10.2.10.2.1.6. Provisionamento das instâncias de soluções disponibilizadas em nuvem;

10.2.10.2.1.7. Todos os parâmetros lógicos necessários, por exemplo, endereços IPv4, DNS, SNMP, NTP, etc.;

10.2.10.3. INSTALAÇÃO

10.2.10.3.1. A fase de instalação consiste das seguintes atividades:

10.2.10.3.2. Desembalagem e inspeção visual;

10.2.10.3.3. Instalação física de equipamentos conforme determinado no projeto executivo;

10.2.10.3.4. Energização dos equipamentos;

10.2.10.3.5. Conexão dos cabos de dados conforme determinado no projeto executivo;

10.2.10.3.6. Verificação da versão do sistema operacional e licenças instaladas;

10.2.10.3.7. Instalação lógica e devido licenciamento exigido;

10.2.10.3.8. Configuração dos acessos aos ambientes fornecidos em nuvem;

10.2.10.3.9. Se necessário, deverá ser realizada a atualização do sistema operacional e ativação de licenças;

10.2.10.3.10. Configuração básica de conectividade IP;

10.2.10.4. CONFIGURAÇÃO

10.2.10.4.1. A fase de configuração consiste em executar as configurações lógicas das facilidades conforme determinado pelo projeto de implantação. Essas atividades compreendem:

10.2.10.4.1.1. Configuração de cada serviço da Plataforma;

10.2.10.4.1.2. Testes específicos de cada serviço da plataforma;

10.2.10.4.1.3. Aceites específicos de cada serviço da plataforma;

10.2.10.4.1.4. Configuração da gestão integrada, dashboards e indicadores;

10.2.10.4.1.5. Aceite da gestão integrada;

10.2.10.5. DOCUMENTAÇÃO

10.2.10.5.1. A fase de documentação consiste na geração do relatório técnico descrevendo todas as configurações realizadas. Esse relatório é a condição da passagem formal da Ativação da Plataforma para a Operação da Plataforma;

10.2.10.6. ENCERRAMENTO

10.2.10.6.1. Para fins de comprovação do serviço de implantação deverão ser entregues:

10.2.10.6.1.1. Documentação que comprove o licenciamento de uso das soluções que compõem a plataforma e todos os seus componentes;

10.2.10.6.1.2. Binários, executáveis, aplicativos para instalação ou link para download das soluções que compõem a plataforma;

10.2.10.6.1.3. Relatório com evidências da execução de todas as fases definidas para o serviço de implantação, integração e as respectivas atividades;

10.2.10.7. DA INICIALIZAÇÃO E PLANEJAMENTO

10.2.10.7.1. Reunião de startup:

10.2.10.7.1.1. Apresentação de cronograma;

10.2.10.7.1.2. Levantamento de requisitos;

10.2.10.7.1.3. Informações de ambiente;

10.2.10.7.1.4. Configuração de políticas para planejamento de implementação e configurações.

10.2.10.7.1.5. Levantamento de informações do ambiente pertinentes ao projeto de implementação;

10.2.10.7.1.6. Alinhamento de requisitos necessários para implementação das soluções;

10.2.10.7.1.7. Definição de papeis e responsabilidades;

10.2.10.7.1.8. Levantamento de políticas e regras necessárias para implementação da solução;

10.2.10.7.1.9. Definição e alinhamento de cronograma para implementação da solução;

10.2.10.7.2. O prazo para entrega do planejamento de implementação das soluções, por parte da CONTRATADA, será de até de 30 (trinta dias) dias corridos da assinatura do contrato e a CET tem até 15 (quinze) dias corridos para dar o aceite no projeto;

10.2.10.8. INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

10.2.10.8.1. A CONTRATADA deve fornecer mão de obra especializada e própria para realizar as seguintes atividades no início do contrato, sendo que a CONTRATADA deverá apresentar relação contendo os nomes dos empregados que trabalharão na execução do contrato e copias de registros dos mesmos junto a empresa, devidamente anotado na carteira de trabalho e previdência social – CTPS. As atividades compreendem:

10.2.10.8.1.1. execução de configurações de forma a refletir o projeto de implantação aprovado pela CET;

10.2.10.8.2. O serviço de implementação preferencialmente será realizado em horário comercial, das 08h00 às 17h00, de segunda a sexta-feira, excetuando-se feriados nacionais, estaduais e municipais da cidade de São Paulo, exceto horários que poderão ser estabelecidos fora de horário comercial e nos finais de semana, a critério da CET;

10.2.10.8.3. Criação de políticas em conjunto com as equipes técnicas e de segurança da informação e infraestrutura da CET.

10.2.10.8.4. O prazo para implementação da solução por parte da CONTRATADA, será de 90 (noventa) dias corridos a partir da assinatura do contrato;

10.2.10.8.5. O serviço de Instalação e Configuração de Plataforma única de solução de gestão de dados será mensurado como atividade única,

tendo sua verificação a partir da estabilização da Solução no ambiente da Companhia de Engenharia de Tráfego - CET, totalmente integrada com os diversos segmentos da rede corporativa.

10.2.10.8.6. O serviço de Instalação e Configuração da Plataforma única de solução de gestão de dados terá seu início a partir da abertura de uma ordem de serviço.

10.2.10.9. EXECUÇÃO

10.2.10.9.1. Embora conste previsto que os trabalhos terão o acompanhamento por parte da equipe técnica da CET, cabe intensificar o entendimento que a CONTRATADA terá exclusiva responsabilidade quando à entrega dos serviços destacados, uma vez que estejam em plenas condições de operação munidos de todos os requisitos fornecidos pela CET e de acordo com os prazos estabelecidos;

11. DAS OBRIGAÇÕES DA CONTRATADA

11.1. A Contratada deverá oferecer garantia e suporte para a solução e suas funcionalidades contratadas pelo período da vigência do contrato. A CONTRATADA deverá prestar Serviços de Manutenção "On Site", para todos os componentes do objeto deste edital, incluindo configuração técnica do produto;

11.2. Disponibilizar profissionais qualificados para a solução fornecida;

11.3. Instalar, configurar e acompanhar os testes de funcionamento antes da entrada de produção dos equipamentos;

11.4. Orientar tecnicamente os responsáveis pela operação dos equipamentos, fornecendo os esclarecimentos necessários ao seu perfeito funcionamento;

11.5. Disponibilizar número de telefone (local ou DDG) para suporte telefônico e abertura de chamados técnicos, ou deverá disponibilizar uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da CET, de modo a assegurar alta disponibilidade do canal de suporte técnico para o Sistema fornecido.

11.6. O registro de chamados deve estar disponível em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados).

11.7. Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o serviço;

11.8. Ao final da abertura de cada atendimento de suporte, a CONTRATADA deverá emitir um ticket do chamado técnico contendo, no mínimo:

11.8.1. Número do chamado;

11.8.2. Data e hora de abertura do chamado;

11.8.3. Previsão de conclusão do atendimento;

11.8.4. Severidade do erro;

11.8.5. Descrição da solicitação.

11.9. A CONTRATADA deverá disponibilizar relatórios de chamados por período, contendo, no mínimo, as seguintes informações:

11.9.1. Número do chamado;

11.9.2. Data e hora de abertura do chamado;

11.9.3. Data e hora do início do tratamento do chamado;

11.9.4. Data e hora de resolução do chamado;

11.9.5. Prazo Total de Início do Tratamento do Chamado (ITC);

11.9.6. Prazo Total de Resolução do Chamado (PRC);

11.9.7. Início do Tratamento do Chamado (ITC) cumprido (Sim/Não);

11.9.8. Prazo para Resolução do Chamado (PRC) cumprido (Sim/Não);

11.9.9. Contato do técnico atendente;

11.9.10. Responsável pelo registro do chamado;

11.9.11. Severidade do chamado;

11.9.12. Descrição da solicitação;

11.9.13. Solução aplicada;

11.10. Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da CET e solicitará autorização para o fechamento deste. Caso a CET não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, a CET fornecerá as pendências relativas ao chamado aberto.

11.11. A CET poderá registrar um número ilimitado de chamados de suporte durante a vigência do Contrato.

11.12. Os atendimentos das ocorrências técnicas devem ser realizados em acordo com os critérios definidos pelos níveis de serviço da descrição abaixo, estando sujeita a CONTRATADA, no caso do descumprimento dos prazos, às sanções especificadas neste documento, os prazos serão contados a partir da abertura do chamado por severidade:

11.12.1. Baixa: problema técnico que gere pouco ou baixo impacto na utilização da solução;

11.12.2. Prazo para atendimento e solução da ocorrência: Até 48 horas corridas;

11.12.3. Média: problema técnico que impeça a utilização parcial de uma funcionalidade, não impedindo por completo seu uso;

11.12.4. Prazo para atendimento e solução da ocorrência: Até 24 horas corridas;

11.12.5. Alta: problema técnico que impeça completamente a utilização de uma funcionalidade;

11.12.6. Prazo para atendimento e solução da ocorrência: Até 12 horas corridas;

11.12.7. Urgente: problema técnico que impeça a utilização da solução em sua totalidade ou paralise algum serviço da CET;

11.12.8. Prazo para atendimento e solução da ocorrência: Até 4 horas corridas;

11.13. Toda infraestrutura necessária para o pleno funcionamento da Plataforma única de Gestão de Dados, tais como: servidores, sistemas operacionais, banco de dados, licenças, entre outros hardwares e softwares necessários, deverá ser disponibilizada em nossos datacenters pela CONTRATADA;

11.14. 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;

11.15. O modelo do equipamento ofertado deverá estar em linha normal de produção e sem previsão de encerramento;

11.16. O tempo máximo de atendimento para os chamados de defeitos deverá ser de 02 (duas) horas e de solução em até 48 (quarenta e oito) horas dependendo de sua severidade) 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 CET, durante o período de garantia;

11.17. A cada visita técnica realizada nas dependências da CET 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 CET;

11.18. Caso a Contratada não consiga recuperar o equipamento em até 72 horas após a abertura do chamado, o equipamento com problema deverá ser substituído por outro novo em até 120 horas após a abertura do chamado;

11.19. A Contratada deverá acompanhar com pessoal in loco o primeiro dia útil de operação do ambiente em produção.

11.20. Prover todo o suporte necessário para a implantação da solução, incluindo interações com os fabricantes das soluções de SGBD, NAS (system file) e principalmente com as equipes de desenvolvimento da CET para integração da solução contratada nas aplicações existentes da CET.

12. OBRIGAÇÕES DA CET

12.1. Nomear gestor e fiscal do contrato para acompanhar e fiscalizar a execução do contrato;

12.2. Encaminhar formalmente à Contratada a demanda de acordo com os critérios técnicos estabelecidos no Termo de Referência;

12.3. Comunicar formalmente à Contratadas quaisquer ocorrências relacionadas a execução do contrato;

12.4. Disponibilizar a infraestrutura de sua responsabilidade para que as soluções contratadas sejam instaladas e configuradas;

13. CONDIÇÕES DE FATURAMENTO

13.1. Para a console de gerenciamento de chaves criptográficas, criptografia de dados para servidores, criptografia de dados via aplicação web, criptografia para compartilhamento seguro de base de dados, solução de gestão de credenciais de alto privilégio deverão ser **faturados integralmente (licença perpétua)** a partir da conclusão do fornecimento e instalação da solução em ambiente da CET.

13.2. Para os módulos de mapeamento e classificação de dados, solução de gestão de identidade e acesso, solução de prevenção à vazamento de dados e painel central de indicadores de segurança, deverão ser **faturados mensalmente (licença mensal)** a partir da conclusão do fornecimento e instalação da solução em ambiente da CET.

13.3. Deverá ser extraído da console de gerenciamento o relatório que demonstre o pleno funcionamento do equipamento e os softwares vinculados para a ação de criptografia nos cenários listados.

13.4. De posse do relatório será deverá ser emitido por parte da CET termo de atesteste a instalação da solução e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente à emissão do termo acima.

13.5. **Os serviços de Suporte Técnico, Manutenção e Garantia** deverão ser atestados através de relatório técnico emitido pela contratada e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia do mês subsequente à prestação do serviço mensal.

13.6. **O Serviço de Operação Assistida** será mensurado como um serviço mensal e deverá ser atestado através de relatório técnico emitido pela contratada e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia do mês subsequente à prestação do serviço;

13.7. **O serviço de Instalação e Configuração** é considerado atividade de execução única e faturado a partir da emissão do Termo de Aceite de Conclusão da Instalação e Configuração e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente à emissão do termo acima e autorização do Gestor do Contrato;

13.8. **O valor relativo ao Treinamento** será faturado a partir da emissão do Termo de Aceite de Conclusão de Treinamento e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente à emissão do termo acima e autorização do Gestor do Contrato.

14. CONDIÇÕES DE PAGAMENTO

14.1. A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CET, através do setor de Expediente, por meio do endereço eletrônico a ser informado oportunamente.

14.2. Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CET disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite, aprovando os serviços prestados.

14.3. O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pela Gerência Financeira 30 (trinta) dias corridos a contar da data de emissão do Termo de Aceite;

14.4. Caso a Nota Fiscal Eletrônica de Serviços contenha divergências com relação ao estabelecido no Instrumento Contratual, a CET 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 CET;

14.5. 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.

15. QUALIFICAÇÃO TÉCNICA

15.1. A LICITANTE deverá apresentar, em seu nome, atestado (s) de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando ter fornecido licenças de uso da solução de natureza semelhante ao objeto.

15.2. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com os serviços de suporte técnico e garantia, por período não inferior a 1(um) ano, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, sendo aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os anos serem ininterruptos.

15.3. Considera-se compatível ou similar ao objeto a comprovação de experiência anterior no fornecimento/licenciamento de solução integrada de segurança da informação, contemplando serviços de manutenção, suporte, treinamento e operação assistida das licenças fornecidas.

15.4. A habilitação da empresa melhor classificada ficará condicionada, ainda, à comprovação das especificações gerais e funcionalidades deste Termo de Referência. Para tanto, deverá executar um Teste de Bancada disponibilizando-a à CET;

15.5. Caso a licitante não atenda as exigências de habilitação do teste de bancada ou qualquer dos documentos de habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda este Edital.

15.6. A licitante melhor classificada deverá prestar apoio e esclarecimentos necessários durante a apresentação e execução do teste de bancada, dando subsídios para que a CET possa homologar a solução proposta.

15.7. O teste de bancada será realizado no endereço da CET a ser informado oportunamente, em horário comercial, de segunda a sexta-feira, das 8h às 12h e das 14h às 17h.

15.8. Após a análise da documentação, respeitada a ordem de classificação do certame, o pregoeiro comunicará, via chat, a licitante que atenda ao edital quanto à documentação habilitatória, para que proceda ao agendamento do teste de bancada junto à área técnica através do e-mail a ser informado oportunamente, conforme disposto a seguir:

15.9. A empresa convocada via chat na sessão do Pregão, terá 2 dias úteis para agendamento através do e-mail ser informado sob pena de desclassificação pelo não cumprimento deste prazo;

15.10. O prazo para início do teste de bancada não será superior a 5 dias úteis após o agendamento;

15.11. Caso a empresa convocada não atenda os prazos, será considerada desclassificada;

15.12. As demais empresas, interessadas em assistir ao teste de bancada, terão dois dias úteis para agendamento através do e-mail a ser informado, a partir da convocação do pregoeiro à empresa que realizará o teste de bancada, indicando até 2 (dois) técnicos ou representantes legais da licitante, devidamente identificados por meio de vínculo contratual ou procuração, como "Técnico de Acompanhamento da Licitante Participante". O não cumprimento deste prazo, ensejará na queda do direito de assistir à realização do teste de bancada;

15.13. Não será permitida a substituição de qualquer Técnico de Acompanhamento da licitante participante sem a autorização prévia da CET;

15.14. Não será permitida a comunicação direta entre qualquer Técnico de Acompanhamento da licitante participante e a Equipe Técnica da licitante convocada. Qualquer comunicação ou questionamento deve ser dirigido unicamente à Equipe Técnica da CET;

15.15. A não observância dessa regra de comunicação poderá causar o descredenciamento da Equipe Técnica da licitante convocada ou de qualquer técnico de acompanhamento da licitante participante;

15.16. O teste de bancada deverá atestar as funcionalidades constantes no Roteiro de Teste de bancada conforme anexo IV;

15.17. A licitante convocada terá um prazo de até 05 (cinco) dias úteis para a completa execução dos testes;

15.18. A licitante convocada deverá prover, integralmente às suas custas, toda a infraestrutura necessária para a completa execução do teste de bancada;

15.19. Fica a critério da licitante optar por demonstrar os testes de funcionalidade, de acordo com o roteiro de teste de bancada, em ambiente local ou virtual (nuvem). Contudo, a execução dos testes deverá ocorrer nas dependências da CET.

15.20. A solução ofertada deverá então ser atualizada para a versão mais atual do software;

15.21. A conformidade com as especificações técnicas e comprovação da execução da solução, de acordo com o roteiro de teste de bancada, ensejará a habilitação da licitante no certame. Do contrário, a reprovação da solução ofertada implicará na desclassificação da licitante;

15.22. Todos os equipamentos e produtos que compõem a amostra da solução ofertada deverão estar acompanhados de seus respectivos programas, CDs, manuais, guias de instalação e demais documentos (físico ou eletrônico) necessários para dirimir dúvidas, a fim de que possam ser realizados procedimentos de verificação de conformidade com as especificações técnicas constantes do item 2 deste Termo de Referência, que serão devolvidos ao representante da empresa convocada;

16. TREINAMENTO

16.1. A Contratada deverá prestar serviços de treinamento aos funcionários indicados pela CET, com as características descritas a seguir:

16.1.1. Deverão ser fornecidos treinamentos oficiais, ministrados por instrutor certificado e autorizado pelo fabricante da solução, para até 10 funcionários, dividido em turmas de no máximo 05 funcionários, agendadas em datas distintas a critério da CET, e em acordo com a CONTRATADA;

16.1.2. Os instrutores deverão possuir experiência em didática, além de possuir certificação comprovada na área de segurança;

16.1.3. Os treinamentos poderão ser fornecidos em turmas abertas, em formato de webinar;

16.1.4. Os treinamentos deverão ser finalizados em até 90 dias após o aceite da instalação/configuração da solução ou em acordo entre as partes.

16.1.5. O treinamento deverá ser ministrado dentro do município de São Paulo em ambiente próprio e dedicado para este fim, caso o treinamento seja realizado fora do município de São Paulo, a CONTRATADA será responsável pelas despesas de transporte, hospedagem e alimentação;

16.1.6. No caso de excepcionalidade de permanência do isolamento social, o treinamento poderá ser fornecido de forma remota;

16.1.7. Os treinamentos deverão ser em idioma português do Brasil;

16.1.8. O material didático poderá ser em idioma português;

16.1.9. Todo o material didático deverá ser repassado em mídia para os alunos;

16.1.10. O conteúdo do treinamento deverá abranger:

16.1.10.1. Apresentação da arquitetura da solução;

16.1.10.2. Visão geral de funcionamento de cada solução;

16.2. O treinamento deverá ser capaz de instruir os alunos administrar e administrar as soluções adquiridas;

Os treinamentos deverão ter no mínimo carga horaria igual ou superior a 40 horas cada;

16.3. Caberá à empresa contratada instalar a plataforma e demais softwares que compõem a solução ou possibilitar o acesso para o treinamento;

16.4. Ao final dos treinamentos, deverá ser emitido certificado de participação;

17. VISTORIA

17.1. Para o correto dimensionamento e elaboração de sua proposta, a licitante poderá visitar o local onde serão executados os serviços, para se inteirar de todos os aspectos referentes à sua execução;

17.2. A visita deverá ser realizada por intermédio de representante legal do licitante que assinará a Declaração de Vistoria, conforme modelo constante no ANEXO II. Esta visita, necessariamente, será acompanhada por técnico do órgão licitante, igualmente habilitado;

17.3. O agendamento deverá ser realizado através do e-mail a ser informado.

17.4. A vistoria poderá ser realizada em até 2 (dois) dias antes do início da Sessão Pública;

17.5. Todos os custos associados com a visita serão de inteira responsabilidade da licitante;

17.6. O licitante que optar pela não realização da visita técnica deverá entregar por ocasião do certame, Declaração em papel timbrado da empresa, assinado por representante legal, afirmando que tinha ciência da possibilidade de fazê-la, mas que, ciente dos riscos e consequências envolvidos, optou por formular a proposta sem realizar a visita técnica que lhe havia sido facultada (ANEXO III).

18. PRAZO DE ENTREGA

18.1. O prazo máximo de entrega de todos os hardwares/softwares que compõem a solução serão de 60 (sessenta) dias corridos, contados a partir da data de abertura de ordem de serviço.

18.2. Prazo máximo para Instalação e configuração (implementação) da solução será de 90 (noventa) dias corridos contados a partir da entrega dos equipamentos, devendo obrigatoriamente ser realizada em finais de semana ou feriados, conforme agendamento da CET.

18.3. Toda a solução deverá ser entregue e instalada no Município de São Paulo;

19. DOCUMENTAÇÃO TÉCNICA

19.1. A licitante, juntamente com seus documentos de proposta deverá fornecer, catálogos ou manuais técnicos de referência ou folders, contendo informações sobre todos os itens que integram a solução ofertada.

19.2. A contratada deverá ser fornecer juntamente com a solução, manuais técnicos de referência, contendo todas as informações sobre os produtos com as instruções para instalação, configuração e operação, preferencialmente em português (Brasil), ou, na inexistência de tradução em português, podem ser escritos em Língua Inglesa;

20. CRONOGRAMA DE IMPLANTAÇÃO E CRONOGRAMA FÍSICO FINANCEIRO

20.1. Cabe observar que a natureza de diversas soluções a serem implementadas é realizar controles e gerir a informação, sendo esse um processo contínuo e dinâmico. Portanto, a implementação é realizada em primeiro lugar disponibilizado as ferramentas com as facilidades contratadas. Após a implementação se inicia a fase de

Operação onde as regras, relatórios, indicadores e políticas são definidas pela Companhia de Engenharia de Tráfego CET e implementada pela CONTRATADA. O cronograma abaixo sugerido trata apenas da disponibilização das soluções de forma que a Companhia de Engenharia de Tráfego CET, através da CONTRATADA, possa iniciar a aplicação de regras, controles e políticas:

MÊS	1				2			
SEMANAS	1	2	3	4	5	6	7	8
1. PLANEJAMENTO E PROJETO								
1.1 Levantamento preliminar de informações	■	■						
1.2 Aprovação/Ajustes do Projeto Executivo		■	■					
2. IMPLEMENTAÇÃO DAS SOLUÇÕES TECNOLÓGICAS								
2.1 Console de Gerenciamento de Chaves Criptográficas			■	■				
2.2 Criptografia para Sistemas de Arquivos de Servidores			■	■				
2.3 Criptografia de Registros em banco de Dados via Aplicações Web			■	■				
2.4 Criptografia para Compartilhamento Seguro de Base de Dados			■	■				
2.5 Módulo de Mapeamento de Classificação de dados.			■	■				
2.6 Solução de gestão de identidade e acesso			■	■				
2.7 Solução de Prevenção de vazamento de dados.			■	■				
2.8 Solução de gestão de credenciais de alto privilégio			■	■				
2.9 Solução de Painel Central de Gerenciamento de Indicadores de Segurança			■	■				
3. Treinamento – Datas a serem definidas posteriormente em função da disponibilidade dos profissionais da Companhia de Engenharia de Tráfego – CET.						■	■	■
4. Início da Operação				■	■	■	■	■

Observações:

1. As soluções, apesar de operarem de forma integrada, podem ser implementadas de forma independente;

2. As licenças, para efeito de utilização, são contabilizadas a partir de sua data de ativação.

CRONOGRAMA DE FÍSICO-FINANCEIRO

ITEM	DESCRIÇÃO DA SOLUÇÃO	MÊS																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	Console de Gerenciamento de Chaves Criptográficas	■																							
2	Criptografia para Sistemas de Arquivos de Servidores	■																							
3	Criptografia de Registros em banco de Dados via Aplicações Web	■																							
4	Criptografia para Compartilhamento Seguro de Base de Dados	■																							
5	Módulo de Mapeamento de Classificação de dados.	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
6	Solução de gestão de identidade e acesso	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
7	Solução de Prevenção de vazamento de dados.	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
8	Solução de gestão de credenciais de alto privilégio	■																							
9	Solução de Painel Central de Gerenciamento de Indicadores de Segurança	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
10	Manutenção e Garantia de Console de Gerenciamento de Chaves Criptográficas	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

11	Manutenção e Garantia para Criptografia para Sistema de Arquivos de Servidores																						
12	Manutenção e Garantia para Criptografia de Registros em Bancos de Dados via Aplicações Web																						
13	Manutenção e garantia para Criptografia de Compartilhamento seguro da base de dados																						
14	Manutenção e Garantia para Solução de gestão de credenciais de alto privilégio																						
15	Serviços de projeto e implementação																						
16	Serviços de operação																						
17	Serviços de treinamento																						

21. CONFIDENCIALIDADE

21.1. 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 CET, durante e após fim do contrato, salvo se houver autorização expressa da CET para divulgação;

21.2. 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 CET. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

22. ACEITE

22.1. Após a instalação e configuração da solução, a equipe técnica da CET emitirá o "Termo de Aceite de Entrega e Instalação" das licenças perpétuas em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo da instalação/configuração (operação) da solução e confirmação que todos os quesitos estão sendo cumpridos conforme o Edital.

22.2. Entende-se pela instalação e configuração, tanto a parte física da solução, configuração lógica de todos os produtos/serviços e testes de todas as regras e procedimentos necessários a operação do serviço.

CONTRATO Nº 073/22

PREGÃO ELETRÔNICO Nº 028/22

EXPEDIENTE Nº 0238/22

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO E INTEGRAÇÃO EM PLATAFORMA ÚNICA DE SOLUÇÃO DE GESTÃO DE SEGURANÇA DE DADOS, EM ATENDIMENTO A LEI 13709/18 - LEI GERAL DE PROTEÇÃO DE DADOS - LGPD, INCLUINDO SUPORTE TÉCNICO, GARANTIA E MANUTENÇÃO DE VERSÕES, OPERAÇÃO ASSISTIDA, SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO, TREINAMENTO, INTEGRAÇÕES NECESSÁRIAS COM SOLUÇÕES DE TERCEIROS PARA ATENDER ÀS DEMANDAS DA CET PELO PERÍODO DE 24 (VINTE E QUATRO) MESES.

MATRIZ DE RISCO

Contrato - Seviços de Segurança da Informação relacionados à Lei 13.709/18- LGPD						
Descrição do Risco	**Descrição do impacto**	**Grau de impacto(de ocorrência do risco)**	**Grau de probablidade (de ocorrência do risco)**	**Grau de severidade (fator multiplicador para aplicação de penalidade)**	**Ação (em caso de ocorrência do risco - medida mitigadora)**	**Atribuição do Risco**
Não disponibilizar o funcionamento do sistema operacional / não ter acesso ao suporte técnico.	Vulnerabilidade na operação com dados pessoais sob Responsabilidade CET	3- Operacional que afete os serviços públicos e imagem da CET	1- Baixo	**3**	ADVERTÊNCIA, para os casos de descumprimento dos itens 6.1; 6.2; 9.2; 9.3. e 11.5. do Anexo I – Termo de Referência.	Contratada

Atraso ou inexecução de impantação e operação e não nomeação de responsáveis	Fragilidade na operação com dados pessoais sob Responsabilidade CET	3-Operacional que afete os serviços públicos e imagem da CET	2-Moderado	**3**	MULTA, devido ao não atendimento ao prazo estipulado nos itens 2.2, 2.3 e 4.1.1.1. deste Contrato e item 10.2.10.8.4. do Anexo I - Termo de Referência	Contratada
Não restabelecimento do sistema de proteção em caso de necessidade (Não execução parcial do contrato)	Comprometimento severo dos sistema protetivos	3-Operacional que afete os serviços públicos e imagem da CET	1- Baixo	**3**	MULTA, devido ao não atendimento ao prazo estipulado nos itens 11.6 e 11.8 do Anexo I - Termo de Referência	Contratada
Não execução de alguns itens constantes na totalidade do contrato	Fragilidade na operação com dados pessoais sob Responsabilidade CET	3-Operacional que afete os serviços públicos e imagem da CET	1- Baixo	**3**	Previsão de penalidade contratual por inexecução parcial do contrato (13.2.1. do Contrato)	Contratada
Inexecução total do contrato	Inexistência de sistema protetivos e descumprimento legal em relação à LGDP	3-Operacional que afete os serviços públicos e imagem da CET	1- Baixo	**3**	Rescisão nos termos do artigo nº 182 do Regulamento Interno de Licitações, Contratos e Convênios - RILCC da **CET**.	Contratada
Níveis de **probabilidade** de ocorrência do risco	1 - Baixo					
	2 - Moderado					
	3 - Alto					
Níveis de **Impacto** em caso de ocorrência do risco	1- Administrativo que pode ser sanado					
	2- Administrativo que comprometa a regularidade do contrato ou operacional que comprometa a gestão					
	3-Operacional que afete os serviços públicos e imagem da CET					

Fator multiplicador de penalidade a ser aplicada ao contrato
*1
*2
*3

Rua Barão de Itapetininga, 18
CEP 01042-000
São Paulo - SP

Fone PABX 3396-8000
www.cetsp.com.br