Governo do Estado de São Paulo
Secretaria de Gestão e Governo Digital
Centro de Licitações e Contratos

TERMO

Nº do Processo: 018.00009726/2024-31

Interessado: Coordenadoria de Tecnologia da Informação e Comunicação - COORTIC

Assunto: Fornecimento de Solução de Gerenciamento de Identidades e Acessos

CONTRATO Nº 035/2024

Secretaria de Gestão e Governo Digital

(Processo Administrativo SEI n°018.00009726/2024-31)

"CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE INFORMÁTICA QUE ENTRE SI CELEBRAM, DE UM LADO O ESTADO DE SÃO PAULO, POR MEIO DA **SECRETARIA DE GESTÃO E GOVERNO DIGITAL - SGGD** E DE OUTRO A **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**."

O ESTADO DE SÃO PAULO, por intermédio da SECRETARIA DE GESTÃO E GOVERNO DIGITAL, com sede no Município de São Paulo, Estado de São Paulo, Bairro Sé, na Avenida Rangel Pestana, 300 – 14º e 16º andar - CEP 01017-911, e por sua **UNIDADE DE GESTÃO DO PROJETO MAIS DIGITAL (UGP)**, neste ato representada pela Senhora **Paula Vitória Pereira**, inscrita no CPF sob o nº 425.823.558-01 no uso da competência conferida pelo Decreto-Lei Estadual nº 233, de 28 de abril de 1970, doravante denominado **CONTRATANTE, e a COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTAO DE SÃO PAULO - PRODESP**, inscrita no CNPJ/MF sob o nº 62.577.929/0001-35, sediada no Município de Taboão da Serra, Estado de São Paulo, Bairro Jardim Goncalves, na Rua Agueda Goncalves, 240, CEP 06.760-900, doravante designada **CONTRATADO**, neste ato representada pelo Presidente, **Senhor Gileno Gurjão Barreto**, inscrito no CPF sob o nº 315.099.595-72 e o Diretor de Relacionamento com Clientes, senhor **Thiago Waltz Alves**, inscrito no CPF sob o nº 950.082.761-15, conforme atos constitutivos e em observância às disposições constantes no Contrato de Empréstimo BID 5579/OC-BR (BR-L1591), amparado no art. 1º, §3º, II, da Lei 14.133/21, e aplicação das normas de contratação previstas nas Políticas de Aquisições do BID, reunidas no documento GN-2349-15 e demais normas da legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente da Contratação Direta nº 01/2024, mediante as condições a seguir enunciadas, de acordo com as subdivisões subsequentes na forma de cláusulas e respectivos itens que compõem este instrumento.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de serviços para fornecimento de solução tecnológica destinada a atender ao **Projeto de Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo**, conforme relacionados no **Termo de Referência (Anexo I)**, na **Especificação de Serviços e Preços" nº E0240240(Anexo II),** na **Planilha de Orçamento (Anexo III)** e **Práticas Proibidas (Anexo IV)** e demais documentos da contratação constantes do processo administrativo em epígrafe.

	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	VALOR UNITÁRIO	QTDE PREVISTA MENSAL	QTDDIAS	VALOR ESTIMADO MENSAL	PARCELA ÚNICA	QTD MESES	DESCONTO INCONDICIONAL	TOTAL ESTIMADO
5.1	**PLATAFORMA COMO SERVIÇO (PaaS) PARA DISPONIBILIZAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E ACESSOS**					**115.678,31**	**109.123.447,66**			**107.705.742,93**
5. 1.1	MIDDLEWARE - PARCELA ÚNICA	UNIDADE DE MIDDLEWARE	1.691,08	64.528,85			109.123.447,66	1	4.193.984,17	104.929.463,49
5. 1.2	MIDDLEWARE - PARCELA MENSAL	UNIDADE DE MIDDLEWARE	1.691,08	62,99		106.521,13		24		2.556.507,12
5.1.3	SERVIÇOS DE GESTÃO DE MIDDLEWARE - AVANÇADO	POR UNIDADE DE GESTÃO / MÊS	9.157,18	1		9.157,18		24		219.772,32

5,2	**INFRAESTRUTURA VIRTUALIZADA ON PREMISES AVANÇADO COM SERVIÇOS DE SUPORTE AVANÇADO - GATEWAY APLICAÇÃO WEB**					**25.192,98**	**400,59**			**605.032,11**
5.2.1	MÁQUINA VIRTUAL CATEGORIA III	SERVIDOR/MÊS	1.967,57	9		17.708,13		24		424.995,12
5.2.2	RECURSOS ADICIONAIS - MEMÓRIA	GRAM/MÊS	56,41	72		4.061,52		24		97.476,48
5.2.3	SERVIÇO DE SUPORTE AVANÇADO	POR SERVIDOR / MÊS	380,37	9		3.423,33		24		82.159,92
5.2.4	ATIVAÇÃO DO SERVIÇO DE SUPORTE AVANÇADO	POR SERVIDOR	44,51	9			400,59	1		400,59
5,3	**FERRAMENTA DE MONITORAMENTO DE APLICAÇÕES**					**14.396,40**	**305,19**			**345.818,79**
5.3.1	MONITORAMENTO DE APLICAÇÕES - SERVIDOR COM ATÉ 16 GB RAM	POR SERVIDOR / DIA	53,32	9	30	14.396,40		24		345.513,60
5.3.2	SERVIÇO DE ATIVAÇÃO - ATIVAÇÃO DE ATÉ 10 SERVIDORES	ATIVAÇÃO ATÉ 10 SERVIDORES	305,19	1			305,19	1		305,19
5,4	**SERVIÇOS DE INSTALAÇÃO - SERVIDOR HTTP**	**POR SERVIDOR**	**925,78**	**9**			**8.332,02**	**1**		**8.332,02**
5,5	**Serviços Técnicos Especializados - ANALISTA DE SUPORTE Nível 2 (Hora Comercial - 08h de 2ª à 6ª das 06:00 às 22:00)**	**HORA HOMEM**	**104,1**	**60**		**6.246,00**		**24**		**149.904,00**
5,6	**Serviços de Manutenção, Suporte Técnico e Garantia**	**UNIDADE**	**212.507,44**	**1**		**212.507,44**		**24**		**5.100.178,56**
TOTAL						**374.021,13**	**104.938.501,29**			**113.915.008,41**

1.2. O presente Termo de Contrato vincula-se à seguinte documentação, que se considera parte integrante deste instrumento, independentemente de transcrição:

1.2.1. O Termo de Referência;

1.2.2. A Autorização de Contratação Direta, e demais documentos que componham a documentação da presente contratação;

1.2.3. A Proposta do Contratado consubstanciada na Especificação de Serviços e Preços" nº E0240240;

1.2.4. O Memorando de Entendimento 1950419 e seus anexos, conforme firmado no processo 018.00000014/2023-75;

1.2.5. Política do Banco sobre Práticas Proibidas;

1.2.6. Demais anexos dos documentos supracitados.

1.3. Na execução e interpretação do contrato, deverão ser observadas as normas do BID, quando houver regulamentação específica quanto ao assunto, cabendo a aplicação subsidiária da Lei 14.133 nos demais pontos em que o regulamento BID não delimitar os parâmetros ou não regular a matéria.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 24 (vinte e quatro) meses, contados da data de sua assinatura, podendo ser prorrogado de acordo com os termos previstos nas Políticas de Aquisições do BID, durante a vigência do Contrato de Empréstimo nº 5579/OC-BR, observadas, no que couber, as disposições dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.2.1. O Contratado poderá se opor à prorrogação de que trata a subdivisão acima, desde que o faça mediante documento escrito, recepcionado pelo Contratante em até 90 (noventa) dias antes do vencimento do contrato ou de cada uma das prorrogações do prazo de vigência.

2.2.2. Dentre outras exigências, a prorrogação de que trata a subdivisão acima é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração e em harmonia com os preços do mercado, conforme pesquisa a ser realizada à época do aditamento pretendido, permitida a negociação com o Contratado, observando-se, ainda, os seguintes requisitos:

a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

c) Seja juntada justificativa, por escrito, de que a Administração mantém interesse na realização do serviço;

d) Haja manifestação expressa do Contratado informando o interesse na prorrogação;

e) Seja comprovado que o Contratado mantém as condições iniciais de habilitação.

2.2.3. O Contratado não tem direito subjetivo à prorrogação contratual, e não poderá pleitear qualquer espécie de indenização em razão da não prorrogação do prazo de vigência contratual por conveniência do Contratante.

2.2.4. Eventuais prorrogações de contrato serão formalizadas mediante celebração de termo aditivo, respeitadas as condições previstas nas Políticas de Aquisições do BID.

2.2.5. Nas eventuais prorrogações contratuais, custos não renováveis já pagos ou amortizados no âmbito da contratação, quando houver, deverão ser eliminados como condição para a prorrogação.

2.2.6. O contrato não poderá ser prorrogado quando o Contratado tiver sido penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

2.2.7. Não obstante o prazo estipulado nesta cláusula, a vigência nos exercícios subsequentes ao da celebração do contrato estará sujeita a condições resolutivas consubstanciadas:

I - na inexistência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício para atender as respectivas despesas, acarretando a extinção do contrato a partir de sua ocorrência; ou

II - na ausência de vantagem para o Contratante na manutenção do contrato, desde que o Contratante comunique ao Contratado a opção pela extinção do contrato com ao menos 2 (dois) meses de antecedência em relação à próxima data de aniversário do contrato, acarretando a extinção do contrato a partir da referida data de aniversário contratual.

2.2.8. Ocorrendo a resolução do contrato, com base em uma das condições resolutivas estipuladas na subdivisão acima desta cláusula, o Contratado não terá direito a qualquer espécie de indenização.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de início, conclusão, entrega, observação e recebimento do objeto, e critérios de medição, constam no Termo de Referência, que constitui parte integrante deste Contrato

3.2. Os serviços serão prestados na forma e condições estabelecidas no Anexo II - “Especificação de Serviços e Preços” e Anexo I - Termo de Referência, que contêm sua descrição, detalhamento, condições, forma e prazo de execução.

3.3. As decisões relativas a serviços, quando solicitados pelo **contratado como condição necessária à execução**, deverão ser tomadas pelo **contratante, e comunicadas** no prazo máximo de 15 (quinze) dias úteis, após o qual, ocorrerá a prorrogação do prazo definido para execução dos serviços, na mesma proporção em que o prejudicar o andamento normal dos trabalhos.

3.4. Todas as informações e comunicações entre o Contratante e o Contratado, deverão ser feitas por escrito. Todas as decisões resultantes de reuniões realizadas entre o Contratante e o Contratado deverão ser formalizadas mediante troca de correspondência.

3.5. Os serviços reexecutados por solicitação do Contratante, que constituam apenas parte dos itens faturáveis, serão cobrados com base nos termos reais de execução e nos valores apontados na “Especificação de Serviços e Preços”, desde que não se trate de reexecução decorrente de culpa ou falha do Contratado, quando constatados vícios de execução ou do material empregado.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação, cessão ou transferência, total ou parcial, do objeto contratual.

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor estimado do presente contrato é de R$ 113.915.008,41 (cento e treze milhões, novecentos e quinze mil, oito reais e quarenta e um centavos), mês de referência novembro/2024, sendo, R$ 105.499.532,98 (cento e cinco milhões, quatrocentos e noventa e nove mil, quinhentos e trinta e dois reais e noventa e oito centavos) para o exercício de 2024, R$ 4.488.253,56 (quatro milhões, quatrocentos e oitenta e oito mil, duzentos e cinquenta e três reais e cinquenta e seis centavos) para o exercício de 2025 e R$ 3.927.221,87 (três milhões, novecentos e vinte e sete mil, duzentos e vinte e um reais e oitenta e sete centavos) para o exercício de 2026, correndo às expensas do Contratante, com recursos financeiros oriundos integralmente do Contrato de Empréstimo nº 5579/OC-BR na dotação orçamentária a seguir: Fonte 175478090, Natureza de Despesa 33904090, PTRES 530157 e Programa de Trabalho 04.126.5302.2656. No valor acima estão incluídos todas as despesas diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação. O valor indicado nesta cláusula é meramente estimativo, de forma que os pagamentos devidos ao Contratado dependerão dos quantitativos efetivamente demandados, medidos e fornecidos.

6. CLÁUSULA SEXTA - RECEBIMENTO E PAGAMENTO

6.1. O prazo para pagamento ao Contratado e demais condições a ele referentes encontram-se definidos abaixo, respeitado o disposto no Termo de Referência, que constitui parte integrante deste Contrato

6.2. O pagamento será efetuado através do Sistema de Administração Financeira de Estados e Municípios – SIAFEM, na Unidade Gestora 533284/53091, Conta Única ou através de depósito em Conta Corrente nº 139595-5, Agência 1897-X, do Banco do Brasil (Decreto nº 55.357 de 18/01/2010), no prazo de **30 (trinta) dias** (Decreto nº 43.914, de 26/03/99), contados da data de entrega da nota fiscal/fatura dos serviços prestados diretamente pela PRODESP.

6.3. A avaliação da execução do objeto observará as disposições sobre os Níveis Mínimos de Serviço – NMS, para aferição da qualidade da prestação dos serviços e eventuais descontos decorrentes.

6.4. Os serviços serão recebidos provisoriamente, no prazo de até 05(cinco) dias, pelo(s) fiscal(is) técnico e administrativo, mediante termo(s) detalhado(s), quando verificado o cumprimento das exigências de caráter técnico e administrativo (Art. 140, I, ‘a‘, da Lei nº 14.133, de 2021, e arts. 17, X, e 18, VI, do Decreto estadual nº 68.220, de 2023).

6.5. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda da Contratada com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

6.6. O fiscal do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

6.7. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à Contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

6.8. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

6.9. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

6.10. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório (Art. 119 c/c art. 140 da Lei nº 14133, de 2021).

6.11. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades cabíveis.

6.12. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

6.13. Os serviços serão recebidos definitivamente no prazo de até 05(cinco) das, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

6.14. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (Decreto estadual nº 68.220, de 2023, art. 18, VII);

6.15. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando ao Contratado, por escrito, as respectivas correções;

6.16. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

6.17. Comunicar ao Contratado para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização; e

6.18. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

6.19. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, se houver parcela incontroversa, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, com a comunicação ao Contratado para emissão de Nota Fiscal no que pertine à parcela incontroversa, para efeito de liquidação e pagamento.

6.20. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela Contratada, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

6.21. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, a contar de seu recebimento pela Administração, na forma desta seção, prorrogáveis por igual período, justificadamente, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

6.22. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como, caso aplicáveis:

6.22.1. o prazo de validade;

6.22.2. a data da emissão;

6.22.3. os dados do contrato e do órgão contratante;

6.22.4. o período respectivo de execução do contrato;

6.22.5. o valor a pagar; e

6.22.6. eventual destaque do valor de retenções tributárias cabíveis.

6.23. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

6.24. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao Sicaf ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

6.25. A Administração deverá realizar consulta ao Sicaf para: a) verificar a manutenção das condições de habilitação exigidas; b) identificar possível razão que impeça a contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas (Instrução Normativa SEGES/MPDG nº 3, de 26 de abril de 2018, c/c Decreto estadual nº 67.608, de 2023).

6.26. Constatando-se, junto ao Sicaf, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

6.27. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

6.28. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

6.29. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso o Contratado não regularize sua situação junto ao Sicaf.

6.30. O pagamento será efetuado no prazo de 30 (trinta) dias, contados da apresentação da nota fiscal ou documento de cobrança equivalente, desde que tenha sido finalizada a liquidação da despesa, conforme seção anterior, nos termos do art. 2º, II, do Decreto estadual nº 67.608, de 2023.

6.31. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente na forma da legislação aplicável (artigo 2º, inciso III, do Decreto estadual nº 67.608, de 2023, c/c o artigo 1º do Decreto estadual nº 32.117, de 1990), bem como incidirão juros moratórios, a razão de 0,5% (meio por cento) ao mês, calculados *pro rata temporis*, em relação ao atraso verificado.

6.32. O pagamento será realizado por meio de ordem bancária, para depósito em conta corrente bancária em nome do Contratado no Banco do Brasil S/A.

6.32.1. Constitui condição para a realização dos pagamentos a inexistência de registros em nome do Contratado no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais– CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pelo Contratado, de que os registros estão suspensos, nos termos do artigo 8º da Lei estadual nº 12.799, de 2008.

6.33. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

6.34. O Contratante poderá, por ocasião do pagamento, efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

6.34.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7. CLÁUSULA SÉTIMA - REAJUSTE

7.1. Os preços inicialmente ajustados são fixos e irreajustáveis pelo prazo de 24(vinte e quatro) meses.

7.2. Após o prazo acima e havendo prorrogação do contrato, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do índice IPC-FIPE – Índice de Preço do Consumidor, exclusivamente para as obrigações iniciadas e concluídas após o período de reajuste.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do Contratante:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e a documentação que o integra;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, a expensas do Contratado;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Comunicar ao Contratado para emissão de Nota Fiscal no que pertine à parcela incontroversa, para efeito de liquidação e pagamento, se houver parcela incontroversa no caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, observando-se as disposições legais pertinentes;

8.1.6. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.8. Cientificar o órgão de representação judicial da Procuradoria Geral do Estado para adoção das medidas cabíveis quando necessária medida judicial diante do descumprimento de obrigações pelo Contratado;

8.1.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, observado o prazo de 10 (dez dias) para decisão, a contar da conclusão da instrução do requerimento, admitida a prorrogação motivada, por igual período, e excepcionada a hipótese de disposição legal ou cláusula contratual que estabeleça prazo específico.

8.1.10. Observar, no tratamento de dados pessoais de profissionais, empregados, prepostos, administradores e/ou sócios do Contratado, a que tenha acesso durante a execução do objeto a que se refere a cláusula primeira deste contrato, as normas legais e regulamentares aplicáveis, em especial, a Lei nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes.

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus profissionais, prepostos ou subordinados.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

9.1. O Contratado deve cumprir todas as obrigações estabelecidas em lei, e aquelas constantes deste Contrato e da documentação que o integra, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto,

observando, ainda, as obrigações a seguir dispostas:

9.1.1. Designar e manter preposto aceito pelo Contratante para representar o Contratado na execução do contrato.

9.1.1.1. A indicação ou a manutenção do preposto do Contratado poderá ser recusada pelo Contratante, desde que devidamente justificada, hipótese em que o Contratado deverá designar outro para o exercício da atividade.

9.1.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

9.1.3. Alocar os profissionais necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, utilizando os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e à legislação de regência;

9.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado diretamente à Administração ou a terceiros em razão da execução do contrato, não excluindo nem reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida na documentação que integra este instrumento, o valor correspondente aos danos sofridos;

9.1.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do Contratante, de agente público que desempenhe(ou) função na contratação ou de fiscal ou gestor do contrato;

9.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastramento Unificado de Fornecedores – Sicaf ou em outros meios eletrônicos hábeis de informações, o Contratado deverá atender a notificação para entregar ao setor responsável pela fiscalização do contrato, no prazo de 5 (cinco) dias úteis, os seguintes documentos: 1) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 2) certidões que comprovem regularidade fiscal perante as Fazendas Estadual/Distrital e/ou Municipal/Distrital do domicílio ou sede do Contratado que tenham sido exigidas para fins de habilitação na documentação que integra este instrumento; 3) Certidão de Regularidade do FGTS – CRF; e 4) Certidão Negativa, ou positiva com efeitos de negativa, de Débitos Trabalhistas – CNDT;

9.1.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, ou Dissídio Coletivo de Trabalho das categorias abrangidas pelo contrato, e por todas as obrigações e encargos trabalhistas, previdenciários, fiscais, sociais, comerciais e os demais previstos em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

9.1.9. Comunicar ao Fiscal do contrato, assim que possível, qualquer ocorrência anormal ou acidente que se verifique no local da execução dos serviços.

9.1.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do objeto.

9.1.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.1.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

9.1.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

9.1.14. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência.

9.1.15. Não permitir a utilização de qualquer trabalho do menor de 16 (dezesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze) anos, nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;

9.1.16. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação direta;

9.1.17. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e incorreta ou inadequada utilização;

9.1.18. Arcar com o ônus decorrente de eventual equívoco no dimensionamento de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros, mas que sejam previsíveis em seu ramo de atividade;

9.1.19. Cumprir as disposições legais e regulamentares federais, estaduais e municipais que interfiram na execução do objeto, bem como as normas de segurança do Contratante;

9.1.20. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo ser exigida do Contratado, inclusive, a capacitação dos técnicos do Contratante ou do novo fornecedor que continuará a execução dos serviços;

9.1.21. Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

9.1.21.1. Considerando que o objeto da contratação envolve a elaboração de projeto relativo a obra imaterial de caráter tecnológico, insuscetível de privilégio, a cessão de todos os direitos patrimoniais a que se refere a subdivisão anterior inclui o fornecimento de todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de qualquer natureza e aplicação da obra, nos termos do § 1º do art. 93 da Lei nº 14.133, de 2021.

9.1.21.2. A cessão de direitos de propriedade intelectual previstos nas Cláusulas anteriores não se aplica à propriedade intelectual da CONTRATADA pré-existente à celebração deste contrato e à propriedade intelectual pertencente a terceiros eventualmente

licenciada à PRODESP, a qual não pode ser cedida.

9.2. Em atendimento à Lei nº 12.846, de 2013, e ao Decreto estadual nº 67.301, de 2022, o Contratado se compromete a conduzir os seus negócios de forma a coibir fraudes, corrupção e quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, de modo que o Contratado não poderá oferecer, dar ou se comprometer a dar a quem quer que seja, tampouco aceitar ou se comprometer a aceitar de quem quer que seja, por conta própria ou por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie relacionados de forma direta ou indireta ao objeto deste contrato, o que deve ser observado, ainda, pelos seus prepostos, colaboradores e eventuais subcontratados, caso permitida a subcontratação.

9.2.1. O descumprimento das obrigações previstas na subdivisão acima poderá submeter o Contratado à extinção unilateral do contrato, a critério do Contratante, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a Lei nº 12.846, de 2013, e o Decreto estadual nº 67.301, de 2022.

9.3. O Contratado obriga-se a não admitir a participação, na execução deste contrato, de:

9.3.1. agente público de órgão ou entidade contratante, ou terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica, nos termos da lei;

9.3.2. pessoa que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função no certame ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, nos termos da lei;

9.3.3. pessoas que se enquadrem nas demais vedações legais previstas nas Políticas de Aquisições do BID.

10. CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. No âmbito da execução do objeto deste contrato, o Contratado deve cumprir a Lei nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes (Lei Geral de Proteção de Dados Pessoais - LGPD), as demais normas legais e regulamentares aplicáveis à proteção de dados pessoais, inclusive regulamentos editados pela Autoridade Nacional de Proteção de Dados, e deve observar as instruções por escrito do Contratante no tratamento de dados pessoais.

10.1.1. O Contratado deve assegurar que o acesso a dados pessoais seja limitado aos empregados, prepostos ou colaboradores que necessitem conhecer/acessar os dados pertinentes, na medida em que sejam estritamente necessários para as finalidades deste contrato, e cumprir a legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade.

10.1.2. Considerando a natureza dos dados tratados, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos no caput do artigo 6º da Lei nº 13.709, de 2018, o Contratado deve adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas aptas a proteger os dados e informações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

10.1.3. Considerando a natureza do tratamento, o Contratado deve, enquanto operador de dados pessoais, implementar medidas técnicas e organizacionais apropriadas para o cumprimento das obrigações do Contratante previstas na Lei nº 13.709, de 2018.

10.1.4. O Contratado deve:

10.1.4.1. notificar o Contratante na primeira oportunidade possível, ao receber requerimento de um titular de dados, na forma prevista no artigo 18 da Lei nº 13.709, de 2018; e

10.1.4.2. quando for o caso, auxiliar o Contratante na elaboração da resposta ao requerimento a que se refere a subdivisão anterior.

10.1.5. O Contratado deve notificar ao Contratante, na primeira oportunidade possível, a ocorrência de incidente de segurança relacionado a dados pessoais, fornecendo informações suficientes para que o Contratante cumpra quaisquer obrigações de comunicar à autoridade nacional e aos titulares dos dados a ocorrência do incidente de segurança sujeita à Lei nº 13.709, de 2018.

10.1.6. O Contratado deve adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança.

10.1.7. O Contratado deve auxiliar o Contratante na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei nº 13.709, de 2018, no âmbito da execução deste Contrato.

10.1.8. Na ocasião do encerramento deste contrato, o Contratado deve, imediatamente, ou, mediante justificativa, em até 10 (dez) dias úteis da data de seu encerramento, devolver todos os dados pessoais ao Contratante ou eliminá-los, conforme decisão do Contratante, inclusive eventuais cópias de dados pessoais tratados no âmbito deste contrato, certificando por escrito, ao Contratante, o cumprimento desta obrigação.

10.1.9. O Contratado deve colocar à disposição do Contratante, conforme solicitado, toda informação necessária para demonstrar o cumprimento do disposto nesta cláusula, e deve permitir auditorias e contribuir com elas, incluindo inspeções, pelo Contratante ou auditor por ele indicado, em relação ao tratamento de dados pessoais.

10.1.10. O Contratado responderá por quaisquer danos, perdas ou prejuízos causados ao Contratante ou a terceiros decorrentes do descumprimento da Lei nº 13.709, de 2018 ou de instruções do Contratante relacionadas a este contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização do Contratante em seu acompanhamento.

10.1.11. Caso o objeto da presente contratação envolva o tratamento de dados pessoais com fundamento no consentimento do titular de que trata o inciso I do artigo 7º da Lei nº 13.709, de 2018, deverão ser observadas pelo Contratado ao longo de toda a vigência do contrato todas as obrigações específicas vinculadas a essa hipótese legal de tratamento de dados pessoais, conforme instruções por escrito do Contratante.

10.1.12. É vedada a transferência de dados pessoais, pelo Contratado, para fora do território do Brasil sem o prévio consentimento, por escrito, do Contratante, e demonstração da observância, pelo Contratado, da adequada proteção desses dados, cabendo ao Contratado o cumprimento de toda a legislação de proteção de dados ou de privacidade nacional e de outro(s) país(es) que for aplicável, a exemplo da Resolução CD/ANPD nº 19/2024, que aprova o Regulamento de Transferência Internacional de Dados.]

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1. Não haverá exigência de garantia contratual da execução.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. Comete infração administrativa, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013 e nas normas e políticas do BID.

12.2. Garantida a prévia defesa, serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

i) **Advertência**, se o Contratado der causa à inexecução parcial do contrato, quando não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

ii) **Impedimento de licitar e contratar**, se praticadas as condutas descritas nas alíneas “b”, “c” e “d” da subdivisão anterior desta cláusula, quando não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii) **Declaração de inidoneidade para licitar ou contratar**, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” da subdivisão anterior desta cláusula, bem como nas alíneas “b”, “c” e “d” da referida subdivisão, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

iv) **Multa:**

(1) Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 90 (noventa) dias;

(2) Moratória de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso injustificado, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para suplementação ou reposição da garantia.

a. O atraso superior à 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do caput do art. 137 da Lei nº 14.133, de 2021.

(3) Compensatória, para as infrações descritas nas alíneas “e” a “h” do item 12.1, de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor do Contrato.

(4) Compensatória, para a inexecução total do contrato prevista na alínea “c” do item 12.1, 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor do Contrato.

(5) Para infração descrita na alínea “b” do item 12.1, a multa será de 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor do Contrato.

(6) Para infrações descritas na alínea “d” do item 12.1, a multa será de 0,5 (cinco décimos por cento) a 30% (trinta por cento) do valor do Contrato.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, § 9º, da Lei nº 14.133, de 2021).

12.4. A multa poderá ser aplicada cumulativamente com as demais sanções previstas neste Contrato (art. 156, § 7º, da Lei nº 14.133, de 2021).

12.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).

12.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, caso exigida na documentação que integra este instrumento, ou, quando for o caso, será cobrada judicialmente (art. 156, § 8º, da Lei nº 14.133, de 2021).

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no *caput* e parágrafos do art. 158 da Lei nº 14.133, de 2021,, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.6. Na aplicação das sanções serão considerados (art. 156, § 1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.7. As sanções são autônomas e a aplicação de uma não exclui a de outra.

12.8. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública, que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159 da Lei nº 14.133, de 2021).

12.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133, de 2021, ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

12.10. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal (Art. 161, da Lei nº 14.133, de 2021).

12.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021..

12.12. O descumprimento de obrigações contratuais pelas partes não será considerado inadimplência se esse fato resultar de um evento de força maior, conforme definido nas condições do contrato.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

13.1. O contrato poderá ser extinto na forma, pelos motivos e com as consequências previstos nos artigos 137 a 139 e 155 a 163 da Lei nº 14.133, de 2021.

13.2. O Contratado reconhece desde já os direitos do Contratante nos casos de extinção por ato unilateral da Administração, prevista no artigo 138 da Lei nº 14.133, de 2021.

13.2.1. O contrato poderá ser extinto por algum dos motivos previstos no artigo 137 da Lei nº 14.133, de 2021, devendo a extinção ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa.

13.2.2. A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará a extinção contratual se não restringir sua capacidade de concluir o contrato.

13.2.2.1. Se a operação societária de que trata a subdivisão acima implicar mudança em pessoa jurídica contratada, deverá ser formalizada alteração subjetiva por termo aditivo.

13.3. O termo de extinção, sempre que possível, será precedido da indicação de:

13.3.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.3.2. Relação dos pagamentos já efetuados e ainda devidos;

13.3.3. Indenizações e multas.

13.4. A extinção do contrato não configura óbice para o reconhecimento de eventual desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput*, da Lei n.º 14.133, de 2021).

13.5. Se for constatada irregularidade no certame ou na execução contratual, caso não seja possível o saneamento, a decisão pelo Contratante sobre a suspensão da execução ou sobre a declaração de nulidade do contrato somente será adotada na hipótese em que se revelar medida de interesse público, observado o disposto nos artigos 147 a 149 da Lei nº 14.133, de 2021, conferindo-se ao Contratado oportunidade para prévia manifestação e participação na instrução.

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

14.1. No presente exercício, as despesas decorrentes desta contratação correrão à conta de recursos específicos consignados no respectivo Orçamento do Estado, na dotação abaixo discriminada:

I.Fonte 175478090

II.Natureza de Despesa 33904090,

III.PTRES 530157

IV.Programa de Trabalho 04.126.5302.2656. 0000

V.UGE 530116

Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao(s) exercício(s) financeiro(s) subsequente(s) será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1. Aplicam-se as Políticas de Aquisições do BID e, nos casos omissos poderão ser aplicadas disposições contidas na Lei nº 14.133, de 2021, e disposições regulamentares pertinentes, e, subsidiariamente, as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021, subsidiariamente às normas e procedimentos previstos nas normas e Políticas de Aquisições do BID.

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Os atos e contratos firmados com o Banco Interamericano de Desenvolvimento (BID), em decorrência do presente instrumento, deverão observar as disposições previstas nas Políticas de Aquisições do BID.

17.2. Para tanto, será garantida a divulgação oportuna das licitações e adjudicações, bem como a disponibilização dos contratos celebrados, em conformidade com os princípios de transparência e igualdade de oportunidades estabelecidos pelas GN2349-15 e GN2350-15.

17.3. A publicação ocorrerá por meio da plataforma online *Development Business* das Nações Unidas (UNDB online) e no site do Banco, conforme exigido pela Política de Aquisições do BID.

17.4. Incumbirá ao Contratante também divulgar o presente instrumento no sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 22 do Decreto estadual nº 68.155, de 2023.

18. CLÁUSULA DÉCIMA OITAVA– FORO

18.1. Fica eleito o Foro da Comarca da Capital do Estado de São Paulo para dirimir quaisquer questões que decorrerem deste Termo de Contrato, que não puderem ser resolvidas na esfera administrativa, conforme art. 92, §1º, da Lei nº 14.133, de 2021.

E assim, por estarem as partes justas e contratadas, foi lavrado o presente instrumento em 01 (uma) via, que, lido e achado conforme pelo Contratado e pelo Contratante, vai por eles assinado para que produza todos os efeitos de Direito, sendo assinado também pelas testemunhas abaixo identificadas.

São Paulo, na data da assinatura digital

_____

PAULA VITÓRIA PEREIRA

SECRETARIA DE GESTÃO E GOVERNO DIGITAL
UNIDADE DE GESTÃO DO PROJETO MAIS DIGITAL

_____

GILENO GURJÃO BARRETO

_____

THIAGO WALTZ ALVES

COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP

TESTEMUNHAS

_____
Shaaly Rodrigues L. de Souza Lima
CPF: 109.886.767-02

_____
Marina Breviglieri Leite
CPF 368.755.438-48

ANEXO I – TERMO DE REFERÊNCIA

1. TÍTULO DO COMPONENTE E DO PROJETO

Componente: Serviços Públicos Digitais

Projeto: Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo

2. IDENTIFICAÇÃO DO CONTRATANTE

Entidade: Secretaria de Gestão e Governo Digital do Estado de São Paulo (SGGD)

Endereço: Av. Rangel Pestana, 300 - 14º e 16º andares - Sé - São Paulo/SP - CEP: 01017-911

3. TÍTULO DO COMPONENTE E DO PROJETO

O Projeto de **Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo,** em implementação na Secretaria de Gestão e Governo Digital do Estado de São Paulo (SGGD), financiado parcialmente com recursos do Banco Interamericano de Desenvolvimento (BID), mediante o contrato de empréstimo BID 5579/OC-BR (BR-L1591), que ampara este Projeto tem por objetivo geral centralizar e padronizar a autenticação e autorização dos acessos às aplicações conectadas a solução Plataforma SP, contribuindo para a prevenção de fraudes e ameaças externas durante o acesso as aplicações web, impedindo a exploração de dados e informações sensíveis e elevando o nível de Segurança das Identidades Digitais do Servidores Públicos de SP.

4. CONTEXTUALIZAÇÃO

A SGGD desempenha um papel crucial no desenvolvimento, modernização e eficiência dos processos organizacionais das instituições do Governo de São Paulo. Um dos seus focos principais é desenvolver e implementar soluções digitais para Órgãos/Entidades do Governo de São Paulo.

Essa transformação digital, por meio da inovação, é considerada um dos principais alicerces tecnológicos para o alcance dos propósitos da SGGD.

Nesse contexto, um dos principais projetos em curso no âmbito da SGGD é a Plataforma SP que tem como objetivo centralizar as atividades executadas pelos servidores públicos relacionadas a disponibilização dos serviços digitais do estado de São Paulo.

A plataforma SP é baseada em dois pilares tecnológicos, a disponibilização de uma plataforma com interface customizada que permita a interoperabilidade com outros sistemas do governo do estado, através de API (Application Programming Interface) e uma solução de gerenciamento de identidades e acessos que é o enfoque desse projeto.

A transformação digital, fenômeno que também marca uma onda de inovação no setor público, migrando diversos serviços para os meios digitais, eleva os riscos relacionados à segurança, ampliando os desafios das entidades públicas e privadas sobre a proteção e privacidade dos dados, que são a matéria-prima para prestação do serviço público. Além disso, algumas normativas governamentais, como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a lei n° 12.965/2014 - Marco Civil da Internet, exigem que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos voltados para segurança da informação.

Esta preocupação fica evidenciada no Decreto n.º 67.799, que instituiu a Estratégia de Governo digital do Governo do Estado de São Paulo, que tem como um dos seus princípios o investimento em desenvolvimento de soluções com enfoque na segurança de dados e informações, conforme podemos observar no inciso VI, do artigo 3º do referido Decreto, in verbis:

Artigo 3° - São princípios da Estratégia de Governo Digital:

.....

VI - Privacidade e Segurança da informação, por meio de contínuo investimento no desenvolvimento de soluções tecnológicas que assegurem a segurança física e lógica de dados e informações;

Contudo, esse processo tem como premissa o controle eficiente dos acessos, bem como definições de perfis e privilégios de acesso para usuários e sistemas sob gerenciamento do governo. Nesse mesmo sentido, faz-se necessário que os órgãos do Governo possuam, com o auxílio de soluções tecnológicas adequadas à segurança, o total gerenciamento sobre as credenciais utilizadas para acessos a sistemas, a visão sobre acessos realizados e a possibilidade de definir regras de segmentação e controle de acessos autorizados e não-autorizados.

No período da pandemia, foi observado um crescimento exponencial de incidentes cibernéticos, que afetaram a disponibilidade de informações, tanto na esfera privada quanto na pública. Neste contexto, é pertinente elencar alguns casos recentes que atingiram sistemas de diversas áreas:

03/11/2020 - Superior Tribunal de Justiça. Dados dos servidores de rede virtualizados do STJ, juntamente com seus arquivos, foram criptografados, inclusive, com tentativa de destruição do ambiente de backup, gerando indisponibilidade de praticamente todos os sistemas de TI do STJ (https://www.conjur.com.br/2021-jun-09/policia-federal-ainda-investigando-ataque-hacker-stj);

28/04/2021 - Tribunal de Justiça do RS. Doze mil servidores de rede perdidos em ataque do tipo ransomware (https://www.cisoadvisor.com.br/tribunal-de-justica-do-rio-grande-do-sul-prejudicado-em-ataque-de-ransomware/);

19/08/2021 - Lojas Renner. Site indisponível, inviabilizando as operações por meio da Internet (https://www.cisoadvisor.com.br/ransomexx-assina-ataque-as-lojas-renner/);

10/12/2021 - Ministério da Saúde. Serviços paralisados, site adulterado, inviabilizando o acesso de informações relativas à pandemia (https://www.cisoadvisor.com.br/ataque-sequestra-dns-e-congela-servicos-do-ministerio-da-saude/);

30/03/2022 - Tribunal Federal da 3ª Região (TRF-3). Todos os serviços prestados indisponíveis (https://www.cisoadvisor.com.br/tribunal-federal-trf3-suspende-atividades-apos-ataque-cibernetico/);

23/06/2022 - Rede FastShop. Atingida por ataque cibernético (https://www.cisoadvisor.com.br/fast-shop-e-atingida-por-um-ataque-cibernetico/);

21/10/2022 - TCE-RS. Ataque Hacker manteve site fora do ar e prazos de atendimento suspensos (https://gauchazh.clicrbs.com.br/geral/noticia/2022/10/tribunal-de-contas-do-estado-segue-com-prazos-suspensos-e-site-fora-do-ar-quase-um-mes-apos-ataque-hacker-cl9ilihtc003f013p1icti7i4.html);

05/01/2023 - Ciberataques a governos subiram 95%, no 2º semestre de 2022 (https://www.cisoadvisor.com.br/ciberataques-a-governos-cresceram-95-no-2o-semestre-de-2022/).

Como consequências comuns dos casos mencionados anteriormente, pode-se destacar a indisponibilidade de serviços, bem como o sequestro e vazamento de informações. Tais incidentes foram possíveis graças a brechas de segurança que viabilizaram o acesso a credenciais administrativas ou a possibilidade de execução de codificação maliciosa não detectada por mecanismos tradicionais de segurança cibernética.

Esse cenário complexo é tratado pela conceituada empresa de consultoria Gartner, no artigo "**Top 7 Trends in Cybersecurity for 2022**", de abril de 2022, em que é feito um alerta para os riscos que as organizações e gestores de informação estão submetidos, e cita a preocupação principal como sendo a "Expansão da superfície de ataque", principalmente causada pelo trabalho remoto, e recomenda que os "líderes de segurança olhem além da abordagem tradicional de monitoramento, detecção e resposta, para uma gama mais ampla de riscos de segurança". E como segunda maior preocupação, a "Defesa de sistemas de identidade", e faz uma

afirmação até surpreendente de que “o mau uso de credenciais é hoje o principal método que hackers usam para acessar sistemas e alcançar seus objetivos”. (https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022).

Segundo o “Gartner Glossary” (https://www.gartner.com/en/glossary), o gerenciamento de identidades e acessos (IAM) é a disciplina que permite que os indivíduos certos acessem os recursos certos, nos momentos certos, pelos motivos certos. O IAM atende à necessidade de missão crítica de garantir o acesso apropriado a recursos em ambientes de tecnologia cada vez mais heterogêneos e atender a requisitos de conformidade cada vez mais rigorosos. O IAM é um empreendimento crucial para qualquer empresa. Está cada vez mais alinhado aos negócios e requer habilidades de negócios, não apenas conhecimento técnico.

Na publicação “2023 Planning Guide for Identity and Access Management”, de outubro de 2022, (https://www.gartner.com/document/4019621), o Gartner afirma que:

“O IAM é fundamental para atividades digitais distribuídas modernas. Os profissionais técnicos de segurança e gerenciamento de riscos devem desenvolver seus roteiros e arquitetura IAM para fornecer segurança de identidade e melhorar a usabilidade e a interoperabilidade dinâmica como parte de suas iniciativas de 2023.”

No estudo “Magic Quadrant for Access Management” de novembro de 2021, o Gartner relata que a disciplina de gerenciamento de acesso (Access Management ou AM) ocupa o primeiro lugar como fonte de confiança na segurança de identidades. O aumento da dependência de identidades para acesso em qualquer lugar, a qualquer hora, exige que o AM seja mais confiável e fácil de adotar.

No estudo citado acima, o Gartner lista que a disciplina de Access Management (AM) deve prover, minimamente, as seguintes capacidades:

Administração de identidades internas e externas, incluindo serviços de sincronização de diretórios;

Self-service de usuários, incluindo interface para usuários finais e de administração com registro, gerenciamento de senhas, gerenciamento de perfil e delegação de administração;

Catálogo de aplicações da sua força de trabalho com login único (SSO);

Autorização e acesso adaptativo com suporte para protocolos modernos, como o Auth 2.0;

Gerenciamento de sessões;

Métodos de autenticação dos usuários, incluindo múltiplo fator de autenticação e login único (SSO);

Integração com políticas de “traga seu próprio dispositivo” (BYOD) e uso de identidades públicas, como contas de média social para acesso; API de controle de acesso para controlar autenticação e autorização para APIs alvo;

Suportar aplicações padrões, incluindo capacidades para acesso rápido, SSO e MFA para SaaS e Aplicações Web, por meio de protocolos modernos, como SAML e OpenID Connect;

Suportar aplicações customizadas, incluindo capacidade para acesso rápido, SSO e MFA, para aplicações web legadas que não suportam protocolos de SSO;

Capacidade analítica, incluindo relatórios, logs e informações analíticas de identidades sobre administração e acesso em tempo de execução.

Segundo estudos da Verizon, as credenciais dos usuários estão constantemente em risco e 72% das brechas de segurança são causadas por credenciais comprometidas (no setor público). Tal fato torna a questão de identidade e o gerenciamento de acesso privilegiado um dos controles de segurança mais críticos, especialmente nos dias de hoje, com ambientes de TI mais complexos e com dados sendo acessados de diferentes localidades e dispositivos (celular, vpn, cloud, web, etc) (https://enterprise.verizon.com/resources/reports/dbir/?utm_campaign=DBIR2017&utm_medium=TW&utm_source=brand).

Uma pesquisa do Forrester Wave de 2018 mostrou que pelo menos 80% dos incidentes de segurança da informação que ocasionaram brechas nos sistemas estão relacionados a vazamento de credenciais válidas (https://www.seguridadar.com/bt/inf-pb-forrester-2018.pdf).

Preocupado com esse aumento drástico e entendendo que a segurança de identidades é o principal vetor de ataque sendo explorado atualmente, o governo federal por meio do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), publicou a recomendação 02/2023 (https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2023/recomendacao-02-2023) que, entre outras sugestões, destacamos:

Implementar o recurso de autenticação de multifator (MFA), quando disponível;

Definir uma política específica de controle de senhas administrativas de sistemas críticos;

Implementar o princípio de privilégio mínimo que garanta que usuários tenham o nível mínimo de acesso necessário para cumprir suas tarefas;

Auditar registros de eventos de login em busca de acessos oriundos de endereços IP estranhos à rotina normal da organização (de outros países, por exemplo), ou feitos em horários incomuns.

Recomendação similar foi feita pelo Forrester Research, em sua pesquisa denominada “Evolve your IAM strategy” (Evolua sua estratégia de IAM), que apresenta quatro estágios fundamentais para programas de IAM (https://www.forrester.com/report/-evolve-your-iam-strategy-for-your-digital-business/RES81861):

Determinar a responsabilidade por todas as áreas funcionais do IAM, identificar e analisar os riscos do IAM, criar orçamentos e construir parcerias em toda a organização;

Atribuir e gerenciar privilégios e autorizações de usuários, fornecer autoatendimento ao usuário e aplicar políticas e fluxos de trabalho adaptáveis, respeitando o princípio de privilégio mínimo;

Autenticação do acesso do usuário, inclusive para usuários privilegiados e identidades não humanas, com monitoramento contínuo para identificar atividades anômalas do usuário;

Gerar eficiências operacionais por meio de automação, configuração, melhoria de processos, rastreamento de ROI e do custo total de propriedade (TCO) para determinar o sucesso do projeto e ajustes orçamentários.

Para ilustrar esse cenário, podemos usar como exemplo o Departamento Estadual de Trânsito de São Paulo (DETRAN-SP), particularmente alvo de fraudes envolvendo comprometimento de credenciais com repercussão na mídia. Em matéria de setembro de 2022, o jornal Folha de São Paulo menciona que “o bando clonava senhas de funcionários do Detran para ter acesso ao sistema. Uma vez dentro, os criminosos, segundo a investigação, incluíam dados falsos e alteravam as informações oficiais” (https://www1.folha.uol.com.br/cotidiano/2022/09/entenda-como-funcionava-o-esquema-de-fraude-no-detran-de-sp.shtml).

Outra matéria, também de 2022, veiculada pelo portal R7 diz que a “a mulher aliciava os funcionários para ceder as senhas de seus cadastros para ter acesso, posteriormente, ao sistema interno que efetua o desbloqueio das multas” (https://noticias.r7.com/sao-paulo/chefe-do-esquema-de-fraudes-do-detran-de-sao-paulo-se-apresenta-a-policia-mas-e-liberada-24062022).

Com a implantação de uma solução similar ao escopo desse projeto, as credenciais dos servidores estariam protegidas e esses casos mencionados acima seriam evitados.

5. PROJETO

Conforme mencionado no tópico 4 - Contextualização, as situações de fraude representam uma preocupação comum nas operações do Governo de São Paulo, exigindo uma abordagem proativa na gestão dos riscos relacionados à segurança de identidades na cibersegurança.

A implementação do **Projeto Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo** oferece camadas adicionais de proteção aos fluxos de trabalho críticos, permitindo a detecção de comportamentos suspeitos, simplificando a autenticação e a auditoria detalhada e reduzindo a exposição de credenciais. Almeja-se, assim, a redução de incidentes de fraude e a promoção de uma cultura de segurança da informação entre os colaboradores.

O Projeto visa colocar em prática o que foi definido como princípio na Estratégia de Governo Digital, demonstrando de forma cabal o comprometimento do Governo de São Paulo com a segurança das identidades digitais dos funcionários públicos, por intermédio do aprimoramento das práticas e tecnologias para proteger ainda mais as informações pessoais e profissionais dos servidores e dos sistemas por eles acessados.

Um dos grandes desafios deste projeto é mitigar o risco de uma autenticação frágil, um convite para problemas de segurança, nesses casos é essencial implementar práticas robustas para proteger sistemas e dados. Uma autenticação frágil pode acarretar diversos problemas significativos, tais como:

Acesso Não Autorizado: Senhas fracas ou autenticação inadequada podem permitir que indivíduos não autorizados acessem sistemas, aplicativos ou dados confidenciais. Isso representa um risco à segurança e à privacidade.

Violação de Dados: Se um invasor obtiver acesso a credenciais de usuário, ele pode explorar essa fraqueza para roubar informações sensíveis, como dados pessoais, financeiros ou comerciais.

Comprometimento de Contas: Uma autenticação fraca torna as contas dos usuários vulneráveis a ataques de força bruta, onde os invasores tentam várias combinações de senhas até obter acesso.

Impacto Financeiro: Se uma conta de usuário for comprometida, os invasores podem realizar transações fraudulentas, causando prejuízos financeiros.

Reputação Danificada: Violações de segurança devido a autenticação frágil podem prejudicar a reputação do Governo e suas entidades, afetando a confiança da população e parceiros.

Conformidade Legal: O Governo de São Paulo segue regulamentações específicas sobre segurança de dados e autenticação. Uma autenticação inadequada pode resultar em não conformidade e penalidades legais junto aos órgãos de controle.

Perda de Produtividade: Se os usuários enfrentarem problemas frequentes de autenticação (por exemplo, redefinindo senhas esquecidas), isso pode afetar a produtividade e indisponibilidade de serviços públicos.

Outro grande problema em manter segura as identidades e credenciais é o controle da autenticação e autorização dos servidores em repositórios distintos, este é um desafio complexo que pretende-se resolver com esse projeto.

Abaixo algumas dificuldades associadas a essa situação:

Fragmentação de Credenciais: quando as credenciais estão espalhadas por vários repositórios, torna-se difícil rastrear e gerenciar quem tem acesso a quais sistemas. A falta de uma visão centralizada dificulta a aplicação consistente de políticas governamentais e de segurança.

Sincronização e Consistência: repositórios distintos podem ter diferentes métodos de autenticação e autorização. Hoje, manter esses métodos sincronizados e consistentes é um desafio, especialmente quando há mudanças nas políticas de governo e de segurança.

Risco de Vazamento de Credenciais: Atualmente, se uma credencial for comprometida em um repositório, ela pode ser usada para acessar outros sistemas. Com isso, a falta de controle centralizado aumenta o risco de vazamento.

Complexidade na Gestão de Acessos: Administradores precisam lidar com várias interfaces e ferramentas para gerenciar permissões. Isso resulta em erros, como concessão excessiva ou negação inadequada de acesso.

Auditoria e Conformidade: Rastrear quem acessou quais sistemas e quando é praticamente impossível, pois as credenciais estão dispersas. A conformidade com regulamentações se torna desafiadora.

Integração com Novos Sistemas: Quando novos sistemas são adicionados, garantir que as credenciais sejam corretamente integradas e controladas se torna extremamente complicado.

Outra questão complexa que se pretende equacionar com o projeto Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo, são as ameaças internas. Colaboradores mal-intencionados ou negligentes representam uma ameaça significativa aos ativos e à integridade dos sistemas do Governo.

Colaboradores Mal-Intencionados: Com acesso privilegiado as aplicações e dados do Governo. Suas motivações podem variar: desde vingança, ganho financeiro até espionagem. Podem realizar ações prejudiciais, como roubo de informações confidenciais ou sabotagem de sistemas.

Colaboradores Negligentes: Nem todas as ameaças internas são intencionais. Servidores negligentes também representam riscos. Ações inadvertidas, como clicar em links maliciosos, compartilhar senhas ou deixar dispositivos desbloqueados, podem comprometer a segurança.

Controles de Acesso Granulares: Implementar controles de acesso granulares é fundamental. Isso significa que os privilégios de acesso devem ser concedidos com base nas funções e responsabilidades específicas de cada servidor.

Princípio do Menor Privilégio: Seguir o princípio do menor privilégio ajuda a mitigar riscos. Os funcionários devem ter apenas os privilégios necessários para realizar suas tarefas. Isso limita o impacto caso suas credenciais sejam comprometidas.

Monitoramento Contínuo: O monitoramento constante das atividades dos servidores é essencial. Registros de log, análise comportamental e alertas de atividades suspeitas ajudam a identificar comportamentos anômalos.

A Gestão de Acessos é um campo dinâmico e multifacetado, repleto de desafios que exigem atenção contínua. A fragilidade na autenticação é como uma brecha na muralha, convidando problemas de segurança. Portanto, a implementação de práticas robustas é imperativa para proteger sistemas e dados sensíveis.

Além disso, o controle descentralizado da autenticação e autorização, disperso em repositórios distintos, é uma teia complexa. A falta de uma visão centralizada dificulta a aplicação consistente de políticas de segurança, tornando a gestão um quebra-cabeça desafiador.

Por fim, as ameaças internas e servidores mal-intencionados ou negligentes podem abrir portas para o caos. Portanto, a implementação do **Projeto de Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo** irá controlar acessos granulares e manter um olhar vigilante e essencial para proteger os ativos e preservar a integridade dos sistemas e dados do Governo de São Paulo, considerando 3 grandes conceitos de Segurança de Identidades:

1 - Gestão de Acessos Centralizados (IGA): Permite a equipe de Gestão de Acessos centralizar a requisição, aprovação, e aprovisionamento de identidades através de regras e perfis ou sob demanda através de fluxos personalizados de requisição em conformidade com regras de governança do Órgão, resultando nos seguintes benefícios:

Processo único de onboarding (entrada) de identidades nas aplicações conectadas no framework de identidades.

Requisições de acessos com workflows e formulários personalizados com regras de negócio.

Processo único de offboarding (saída) de identidades nas aplicações conectadas no framework de identidades.

Processo automatizado para movimentação entre áreas.

Framework de identidades único para serem utilizados pelos desenvolvedores das aplicações baseado em padrões reconhecidos de mercado.

Redução no tempo de aprovisionamento de direitos nos sistemas integrados.

Diminuição na superfície de ataque devido a concessão de acessos precisa e somente no tempo necessário.

Melhor experiência para o Servidores Públicos do Estado com processos bem definidos e ágeis sobre Gestão de Acessos.

Melhor experiência para os cidadãos do Estado, pois os colaboradores terão os acessos em tempo para atender suas demandas.

2 - Autenticação e Autorização Centralizada: Permite a equipe de Gestão de Acessos centralizar e ter um ponto único para autenticação e autorização das aplicações conectadas na Plataforma SP, utilizando padrões de mercado e o GOV.BR como fonte única de autenticação, resultando nos seguintes benefícios:

Framework de identidades integrado ao GOV.BR para autenticação única.

Onboarding rápido para novas aplicações no sistema de autenticação e autorização pois é baseado em padrões abertos de mercado.

Segurança na autenticação devido a confiabilidade de uma base única e não múltiplas bases de autenticação.

Parte estruturante de uma visão unificada com o INTEGRADORSP (https://integrador.sp.gov.br/) e IDPSP (https://idp.sp.gov.br) para gestão de acessos em APIs.

Enriquecimento de perfis para autorização nos sistemas integrados, além de informações provenientes do GOV.BR

3 - Monitoração e Prevenção de Fraudes com Inteligência Artificial: Permite a equipe de Gestão de Acessos monitorar, alertar e mitigar comportamentos anômalos, resultando nos seguintes benefícios:

Autenticação baseada em IA para o comportamento dos usuários, trazendo uma visão de risco para cada autenticação.

Possibilidade de adicionar novos fatores de autenticação, inclusive métodos passwordless, caso seja necessária uma verificação adicional, de forma dinâmica baseada nos riscos

6. ABRANGÊNCIA DO PROJETO

Considerando a relevância do projeto, no que tange a disponibilização de uma solução que permita a gestão eficaz das identidades e acessos dos servidores públicos do estado de São Paulo, entende-se que a princípio, todos os 590.000 Servidores Públicos do Estado de São Paulo vinculados a mais de 69 órgãos, devem ter suas credenciais e acessos protegidos contra-ataques maliciosos, roubos e possíveis fraudes.

Contudo, com vistas a utilização racional dos recursos públicos, a SGGD definiu como parâmetro a disponibilização dessa solução, em um primeiro momento, para os servidores que no desempenhar das suas atividades utilizarão diretamente a plataforma SP ou um dos sistemas governamentais que vão interoperabilizar com a Plataforma, entende-se que esses servidores são mais expostos aos ataques e fraudes.

Com base nesse critério, o **Projeto Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo** vai abranger 285.000 servidores, considerando a proposta de divisão elencada abaixo:

ENTIDADE SECRETARIA	/TOTAL SERVIDORES PÚBLICOS	% SERVIDORES PÚBLICOS ATENDIDOS	SERVIDORES PÚBLICOS ATENDIDOS
CASA CIVIL	1.015	30%	305
CGE	190	40%	76
PGE	1.445	40%	578
SAA	3.663	40%	1465
SAP	34.062	30%	10.219
SCEC	1.171	20%	234
SCTI	38.227	40%	15.291
SDE	22.655	60%	13.518
SDPCD	79	41%	32
SDUH	170	30%	51
SECOM	438	30%	131
SEDS	546	60%	328
SEE	296.893	30%	118.699
SERT	1	100%	1
SES	48.097	40%	19.291
SESP	415	40%	166
SFP	5.674	60%	3.404
SGGD	9.059	60%	5.435
SGRI	158	30%	47
SJC	12.134	37%	4.453
SMAIL	4.674	50%	2.344
SPI	264	28%	75
SPM	88	60%	53
SSP	109.526	81%	88.691
STM	256	33%	84
STV	85	33%	28
-	590.985	-	285.000

7. MARCO NORMATIVO

POLÍTICA DE CONTRATAÇÃO DO BID: GN 2349-15 - POLÍTICAS PARA AQUISIÇÃO DE BENS E CONTRATAÇÃO DE OBRAS E SERVIÇOS QUE NÃO SÃO DE CONSULTORIA

Decreto Estadual 67.799/2023 – Estratégia de Governo Digital do Estado de São Paulo.

8. OBJETO

O objeto dessa contratação é o fornecimento de uma solução tecnológica para atender o **Projeto de Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo**, conforme as especificações contidas neste Termo de Referência.

A solução tecnológica garantirá o correto funcionamento da plataforma SP, no tocante a gestão de identidades e acessos, por intermédio da troca de dados de forma segura entre seus diversos módulos, além de disponibilizar em um único local a autenticação, autorização e segurança das identidades para aplicações e servidores públicos.

A solução deverá suportar 285.000 (duzentos e oitenta e cinco mil) servidores públicos que no desempenho das suas atividades utiliza diretamente a Plataforma SP ou um dos sistemas governamentais que vão interoperabilizar com a plataforma.

A contratação terá vigência de 24 (vinte e quatro) meses contados a partir da data da sua assinatura, podendo ser prorrogado por períodos e sucessivos durante a vigência do contrato de empréstimo (5579/OC-BR).

Na hipótese de haver necessidade de aumentar a estrutura com vistas a suportar uma maior quantidade superior a 285.000 (duzentos e oitenta e cinco mil) servidores públicos, a contratante poderá estabelecer um montante adicional, mediante aditivo contratual, respeitados os limites legais. Não havendo este aditamento contratual, o contrato terá seu encerramento antecipado.

9. REQUISITOS TÉCNICOS QUE COMPÕE A SOLUÇÃO

Os requisitos técnicos definidos nesta contratação têm como finalidade desenvolver, personalizar e disponibilizar em um único local a autenticação, autorização e segurança das identidades para aplicações e servidores públicos do Estado de São Paulo, tendo como prerrogativa básica as seguintes necessidades e serviços:

Integração com o provedor de identidades do Governo Federal (https://acesso.gov.br/roteiro-tecnico), também conhecido como GOV.BR, um provedor seguro para autenticação, com seus diversos níveis de segurança (prata, bronze e ouro) adicionando camadas de validação para obtenção dos selos e liberação de serviços com maior criticidade, já utilizado e provado em sistemas críticos e bancos do governo federal.

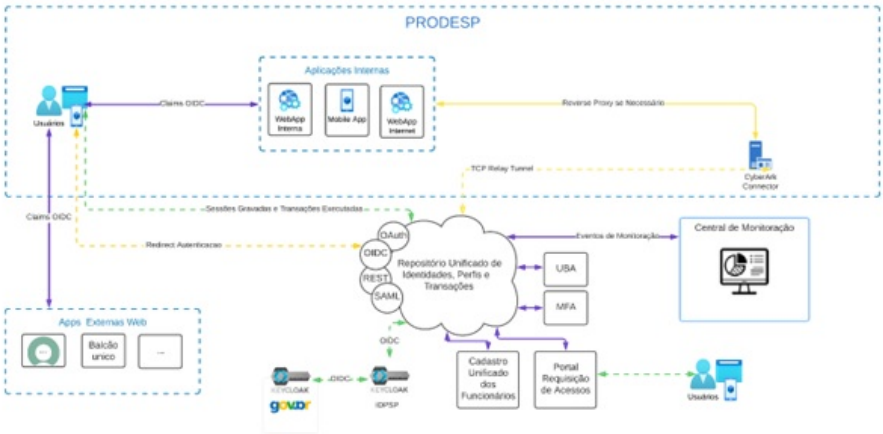
Oferecer e atuar como um orquestrador de permissionamentos nas aplicações do Estado de São Paulo, sendo o ponto central para requisição, revogação e concessão automatizada de perfis e transações nas aplicações integradas com a Plataforma SP. Deve prover em tempo de autenticação e durante a sessão os direitos/autorizações das identidades provenientes de seu repositório centralizado, incluindo informações para autorização do acesso, bem como informações dos perfis do usuário para serem utilizados pelas aplicações integradas na ativação de funcionalidades específicas para cada perfil. A solução deve permitir a customização das informações incluídas tanto na autenticação como no acesso via APIs.

Disponibilizar a criação de fluxos de trabalho personalizados para requisições e aprovações de perfis e transações, de maneira intuitiva, sem a necessidade de codificação, utilizando padrões abertos de mercado. Um dos pontos importantes desta capacidade é a de aumentar a eficiência operacional do Estado e a segurança dos acessos, entregando somente os direitos necessários e no tempo necessário, suportando um conceito de segurança da informação amplamente difundido, chamado confiança zero (Zero Trust).

Combater fraudes internas e externas que possam ocorrer em seus sistemas tecnológicos, para dar este suporte e combater tais eventos os serviços devem prover de auditoria detalhada de cada acesso as aplicações do Estado, de maneira textual, indexada e também visual, com imagens de cada ação das aplicações críticas. Este serviço dará suporte às áreas de auditoria em suas diligências para obter provas com maior facilidade e rapidez além de gerar evidências de transações de negócio que nativamente não são geradas por deficiência da aplicação.

Diretamente atrelado a necessidade anterior de combate a fraudes e segurança dos sistemas, espera-se que os serviços técnicos especializados disponibilize à SGGD informações geradas por algoritmos de aprendizado de máquina, suportando um tema muito em voga no mercado chamado IA (Inteligência Artificial), onde reconheça padrões de autenticação de cada identidade e a partir deste reconhecimento, calcule riscos de cada autenticação sendo capaz de sinalizar ações, tal como, bloquear uma autenticação devido um desvio de comportamento (horários, dias da semana, tipo de navegador, tipo de sistema operacional, localizações, falhas consecutivas de autenticação, dentre outros atributos).

Destacamos abaixo o diagrama da arquitetura necessária para o **Projeto de Gestão de Acessos e Autenticação Centralizada dos Servidores Públicos de São Paulo**.



DETALHAMENTO DOS REQUISITOS TÉCNICOS QUE DEVEM COMPOR A SOLUÇÃO

10.1. **GESTÃO DE ACESSOS COM PORTAL SINGLE SIGN-ON (SSO) E AUTENTICAÇÃO MULTIFATOR (MFA)**

A solução deve prover um catálogo de aplicações Web com modelos de configuração de Single Sign-On (SSO) abrangendo as aplicações mais conhecidas de mercado, com a finalidade de facilitar a configuração destas integrações.

A solução deve permitir a configuração do SSO para aplicações Web minimamente através dos seguintes protocolos e métodos:

SAML 2.0.

Oauth 2.0 modo cliente.

WS-Federation.

OpenID connect.

NTLM.

Oauth 2.0 modo server.

HTTP Basic.

A solução deve oferecer suporte para a personalização das repostas SAML, como por exemplo, mapear atributos dos diretórios para atributos SAML, ter a capacidade de incluir lógicas complexas para manipulação das repostas SAML e possibilitar a visualização da reposta SAML configurada antes de sua implantação.

A solução deve suportar métodos de MFA distintos e configuráveis por perfis que possam ser associados a grupos de usuários distintos, incluindo no mínimo os desafios:
Senha pessoal
E-mail
SMS
Token virtual TOTP
Token físico (FIDO2 ou equivalente)
Aplicativo de acesso
Passkeys

A solução deve suportar a organização dos desafios em 2 níveis, com o usuário respondendo com sucesso ao menos uma opção de cada nível configurada no respectivo perfil de autenticação.

A solução deve contemplar tecnologia com algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados para cálculo de risco.

A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos:

Geo Velocidade: mede a velocidade de deslocamento do login, comparando a localização do último login com a atual, evitando “viagens impossíveis”, e traçando o comportamento do usuário neste quesito, por exemplo, pessoas que viajam muito podem ter uma pontuação de risco baixa mesmo que sua Geo Velocidade seja maior que pessoas que não viajam.

Geo Localização: mede o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual.

Dia da Semana: mede o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.

Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.

Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual.

Falhas de login consecutivas: mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual.

O cálculo do risco pelo motor de aprendizado de máquina, da tecnologia utilizada pelo serviço a ser prestado, não utilize somente um atributo fora da normalidade reconhecida anteriormente pelo mesmo, mas sim em uma única autenticação calcule o risco baseado em todos os atributos citados acima e suas anormalidades em uma única autenticação. Cabe exemplificar: uma identidade tem por costume realizar sua autenticação as 9,10 e 11 da manhã, nas aplicações A e B, nas segundas-feiras e quintas-feiras, utilizando um dispositivo Android, das cidades de Brasília e São Paulo. Em futuro login acaba realizando a autenticação as 14 horas (fora do seu horário regular), na aplicação A, em um sábado (não é um dia da semana usual para esta identidade), de um dipositivo IOS (também não usual), da cidade de Brasília. O motor de aprendizado de máquina deve ter a capacidade de reconhecer estes três desvios de comportamento e retornar um risco calculado (alto, médio, baixo ou sem risco) referente a mesma.

A solução deve disponibilizar múltiplo fator de autenticação para casos de uso com capacidade de interpretação de risco adaptativo baseados em algoritmos de aprendizado de máquina e reconhecimento de comportamentos temporais para cada identidade (dias da semana e horários), o mesmo calculado antes da autenticação para tomada de ações antes da materialização da autenticação.

A solução deve disponibilizar a personalização das faixas de pontuação (0 a 100) para os administradores para, no mínimo, as categorias:
Sem risco.
Risco Baixo.
Risco Médio.
Risco Alto.

A solução deve prover para os administradores a personalização da influência na medição do risco para cada atributo citado neste item. Cabe exemplificar, para a SGGD a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco.

O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator (MFA) de autenticação e Single Sign-On (SSO) que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:
Requisitar múltiplos fatores de autenticação de forma dinâmica.
Permitir o login sem o uso de múltiplos fatores.
Negar a autenticação.

A solução deve prover para os administradores a capacidade de explorar os dados históricos através de dasboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.

A solução deve prover visualizações gráficas de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis

A solução deve ser capaz de demostrar e exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações para consultas posteriores.

A solução deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud, Check Point ThreatCloud, CrowdStrike Falcon ZTA e Forescout.

A solução deve viabilizar interface para envio de alertas de forma automatizada, indicando, no mínimo:
E-mail com conteúdo do alerta.
Webhooks (por exemplo: envio de mensagem para um canal do Microsoft Teams ou Slack).

A solução deve disponibilizar dashboards pré-configurados com informações e gráficos com as seguintes características:
Utilização do Motor de Análise do Comportamento dos Usuários.
Comportamento dos usuários na utilização das aplicações.
Visão sobre a segurança das aplicações.
Mapa com a geolocalização das autenticações.
Visão sobre o comportamento dos endpoints (mobile e computadores).
Visão sobre o comportamento das identidades.

A solução deve disponibilizar configuração de dashboards personalizados.

A solução deve disponibilizar compartilhamento dos dashboards com outros usuários.

Para cada caso de uso ou conjunto de casos de uso de múltiplo fator de autenticação citados, o Serviço deve ser capaz de identificar os atributos de contexto de cada autenticação para disponibilizar os melhores métodos definidos para a autenticação, contendo minimamente:
Endereçamento IP.
Dia da Semana.
Datas específicas.
Janelas de tempo entre duas datas.
Janelas de tempo entre horários (por exemplo: horário comercial).
Tipo do Sistema Operacional.
Tipo do Browser.
Perfis configurados.
País que está sendo realizado o acesso.
Se é um dispositivo gerenciado.
Autenticação via certificado.
Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários.

10.2. ACESSO SEGURO SEM VPN PARA APLICAÇÕES WEB

A solução deve prover tecnologia embarcada para intermediar o SSO em aplicações web sitiadas no datacenter da Prodesp ou de seus clientes sem a necessidade de expor estas aplicações para a internet ou uso de VPN e deve suportar os mesmos métodos e protocolos do item anterior.

A solução deve prover a nuvem para intermediar o fluxo de dados entre a aplicação sitiada no datacenter da Prodesp ou de seus clientes e o navegador personalizado e configurado que acessa a aplicação, com a finalidade de não expor diretamente o acesso a esta aplicação.

A solução deve realizar a importação de certificados digitais para prover personalização do domínio acessado via nuvem.

Caso a SGGD não queira utilizar um domínio próprio para a publicação o serviço deve indicar um nome de DNS em sua nuvem para acesso.

A solução deve disponibilizar o bloqueio de acesso a aplicação com o IP inicial da conexão, caso o mesmo mude, e deve pedir reautenticação ao usuário.

A solução deve oferecer a opção de respeitar ou não o tempo de expiração do cookie de autenticação gerado na autenticação pela nuvem disponibilizada e não da aplicação.

A solução deve oferecer a possibilidade de reescrever a URL externa com a URL interna da aplicação, pois muitas aplicações possuem este tipo de informação hardcoded em seu código HTML.

A componente sitiado no datacenter da Prodesp ou de seu cliente terá capacidade de fail over e load balance nativamente sem a necessidade de balanceadores de carga.

10.3. ORQUESTRAÇÃO DO APROVISIONAMENTO DE IDENTIDADES

A solução deve provisionar identidades usando os protocolos modernos REST ou SCIM.

A solução deve prover não somente a capacidade de autenticação, mas também o aprovisionamento /desprovisionamento de identidades em aplicações SaaS, contemplando, no mínimo, o aprovisionamento com modelos prontos no catálogo para:
Office 365.
Google Workspaces.
Azure.
Amazon Web Services.
Docusign.
Salesforce.
ServiceNow.
Zendesk.

A solução deve oferecer REST API para as seguintes operações:
Operações de criação, leitura, atualização e deleção em objetos do tipo usuário.
Operações de criação, leitura, atualização e deleção em objetos do tipo grupo.

A solução deve realizar o aprovisionamento em aplicações que suportem interfaces gerenciamento de identidades entre domínios (SCIM), padrão de mercado para aplicações entregues no modelo SaaS para aprovisionamento de identidades.

A solução deve ser capaz de provisionar com base nas funções (perfis) já configuradas. Por exemplo: se a identidade fizer parte de uma função de funcionário, ela será criada no diretório do Active Directory e também na aplicação SalesForce com as licenças aplicadas e funções e grupos atribuídos nos dois aplicativos.

A solução deve ser capaz de reconhecer alterações em grupos do Active Directory e com base nessas alterações, fazer o provisionamento automaticamente em funções nas aplicações conectadas.

A solução deve ser a capaz de transformar dados e atributos para atender aos requisitos de negócios e fornecer os dados necessários nas aplicações conectadas.

A solução deve oferecer aos usuários a capacidade de solicitar acessos para aplicativos com fluxos de aprovação configuráveis.

A solução deve ser a capaz de desprovisionar as identidades nos aplicativos automaticamente com base nas mudanças nas funções ou na desativação de uma conta de usuário com a opção de excluir ou desativar a identidade no aplicativo conectado.

A solução deve oferecer o sincronismo completo ou incremental das identidades e permissões nas aplicações conectadas. E ainda deve ser capaz de fornecer relatórios completos sobre estes sincronismos com as falhas e modificações ocorridas, os mesmos devem ser acessíveis por interface web e também envio automático por email na finalização de um ciclo de sincronismo.

10.4. ORQUESTRAÇÃO DE REQUISIÇÕES APROVAÇÕES E APROVISIONAMENTO POR WORKFLOWS

A solução deve criar e disponibilizar um módulo de criação de workflows no estilo no-code, ou seja, sem a necessidade de nenhum tipo de codificação utilizando somente parametrizações, para integração e automação do fluxo de informação de identidades, assim facilitando a integração com sistemas de ITSM, provisionamento de identidades em aplicações, tomadas de decisão, transformação e agregação de dados.

Para a criação de workflows o serviço deve ser a capaz de criar de formulários de entradas de dados totalmente personalizáveis, sem necessidade de codificação. Os formulários podem ser utilizados em qualquer parte do fluxo de trabalho visando melhorar a tomada de decisão e também fornecer mais informações de forma manual durante a execução de um workflow.

Para criação de workflows o serviço deve oferecer uma biblioteca com chamadas de APIs pré configuradas para as principais soluções de mercado, citando como exemplo, AWS, Azure, GCP, ServiceNow, Slack, soluções de Recursos Humanos dentre outros.

Para de criação de workflows o serviço deve realizar a importação de APIs que não estão presentes no catálogo através do formato OpenAPI o qual é um padrão de mercado extremamente difundido para definição de APIs.

A criação de workflows deve ser WEB.

A solução de workflow deve também atuar como um gateway SCIM (System for Cross Domain Identity Management), padrão de mercado para gestão de identidades entre aplicações. Deve ser capaz de receber chamadas do tipo SCIM e converter em chamadas web API para aplicações que não suportem chamadas SCIM nativamente, funcionando como um tradutor de qualquer chamada SCIM para web APIs e vice-versa.

A solução deve disponibilizar um banco de dados interno com acesso via Workflows para persistência e consulta de dados dos wokflows em execução.

A solução deve suportar a criação de fluxos para a gestão automática dos perfis de acesso, incluindo formulários de solicitação de acesso pelos usuários que disparam notificação para os aprovadores responsáveis de cada perfil.

A solução deve segregar a visualização dos formulários de solicitação e de aprovação apenas para os colaboradores associados a perfis específicos, podendo estes serem separados por um nível de agregação dito “Organizações”.

10.5. REQUISITOS GERAIS

A Solução ofertada deverá suportar até 30.000 autenticações simultâneas por minuto e disponibilizar tokens ativos para todos os usuários licenciados nesta oferta.

Caso a Solução ofertada necessite de conectores no ambiente da SGGD e Órgãos Vinculados, deverá ser compatível com servidores de virtualização de mercado e sistemas operacionais Windows ou Linux (padrão utilizado no Estado de São Paulo) de forma exclusiva.

10.6. MONITORAMENTO DA SOLUÇÃO

Serviço de monitoramento da infraestrutura, contemplando a disponibilização de indicadores, tais como: indicadores de utilização de processamento, memória, disco e as respostas das portas do servidor, de forma a auxiliar no acompanhamento da saúde do ambiente (produção/homologação);

A solução auxilia na identificação da causa raiz de problemas de desempenho, por meio do monitoramento profundo da aplicação, em seus diversos aspectos, tais como: URLs, classes, métodos, erros, exceções, queries, dump de memória, entre outros, além de identificar a origem de problemas de desempenho ou disponibilidade, medindo tanto o tempo de execução, como também os tempos de sincronização, I/O, CPU, garbage collection, entre outros;

10.7. IMPLANTAÇÃO E IMPLEMENTAÇÃO DO PROJETO

O Serviço de Implantação e Implementação do projeto deve oferecer:
Mobilização das equipes participantes do projeto;
Elaboração dos termos de início e encerramento do projeto;
Elaboração de cronograma de atividades elaborado em conjunto com a SGGD;
Organização de reuniões e interação com as partes interessadas;
Relatório periódico de status;
Monitoramento e controle do projeto quanto à sua evolução, tratando eventuais mudanças;
Elaboração de termos de aceite para formalização de entregas;
O Serviço de implementação do projeto e de soluções necessárias deve fornecer todo o apoio técnico e gerencial necessário para o início do projeto, compreendendo atividades especializadas de implementação e customização de políticas conectores e alertas;
Disponibilizar e configurar o serviço de integração de aplicações nativas do tipo SAML e/ou OpenID, para habilitação de SSO garantindo a relação de confiança entre a solução e as aplicações de forma segura;
O serviço poderá desenvolver relatórios técnicos e gerenciais relacionados à implementação do projeto, como exemplo, relatório de status report, relatórios de riscos e problemas e relatório de conclusão do projeto;
A ativação inicial do licenciamento relacionado às soluções contratadas;
Instalação e parametrização dos componentes embarcados na soluções contratadas;
Configuração inicial de conectores, políticas e alertas.

10.8. MANUTENÇÃO, SUPORTE TÉCNICO E GARANTIA

Administração das Ferramentas: Oferecer administração centralizada da ferramenta, permitindo acesso à console para gestão e monitoramento eficaz de identidades, papéis e aplicações. Prestar auxílio na configuração de políticas de autenticação, garantindo a segurança contínua das suas identidades. Suportar a aplicação e políticas de acesso.

Desenvolvimento de Relatórios: Desenvolver relatórios técnicos e gerenciais contemplando a auditoria de alterações de políticas, estatística de usuários com fatores de risco e acessos a aplicações para fornecer insights sobre a segurança das identidades.

Cadastro, Autorização e Manutenção de Aplicações: Auxiliar no cadastro, manutenção e autorização de aplicações na solução, incluindo orientação para construção de fluxos de automação e integração de ciclo de vida utilizando SCIM.

Manutenção Preventiva e Corretiva: Fornecer atualizações regulares do software conforme disponibilização de novas versões do fabricante para garantir a segurança e o desempenho otimizado do sistema. Resolução de problemas emergentes por meio de correções de bugs e patches de segurança. Revisões periódicas de desempenho e integridade do sistema para identificar e resolver possíveis problemas antes que afetem a operação.

Suporte Técnico Especializado: Disponibilizar equipe de suporte técnico dedicada e altamente qualificada, disponível para responder a consultas e resolver problemas técnicos de forma rápida e eficiente. Utilização de ferramenta de ITSM para abertura de chamados garantindo uma resposta rápida e eficaz às necessidades. Suporte remoto para diagnóstico de problemas e solução de questões técnicas sem a necessidade de intervenção presencial, garantindo uma resolução mais ágil dos problemas.

10.9. REQUISITOS GERAIS

A solução deve estar em conformidade com os requerimentos da ISO 27001:2013 que visa estabelecer, implementar, manter e melhorar continuamente uma solução com foco em gestão de segurança da informação.

A solução deve considerar a utilização de tecnologia em nuvem no formato de entrega SaaS, com possibilidade de integração com o ambiente on-premises.

Essa tecnologia deve possuir certificação SOC 2 Type 2, padrão de mercado para tecnologia em nuvem do tipo SaaS.

A tecnologia ofertada juntamente aos serviços deve estar minimamente em processo de certificação do Fedramp do tipo "High", com a finalidade de comprovar os mais altos níveis de segurança em sua nuvem pública. O Fedramp é uma das certificações de segurança com o mais alto nível de exigência de boas práticas em gerenciamento de risco de segurança cibernética para produtos e serviços em nuvem usados por agências federais dos EUA, sendo uma excelente referência para o setor privado e público de outros países.

A solução deve sinalizar status de cada ponto de presença regional com informações de incidentes atuais e antigos.

A solução deve disponibilizar REST APIs detalhadamente documentadas no website do fabricante da tecnologia ofertada juntamente aos serviços, estas APIs devem fornecer minimamente as funcionalidades de gestão das identidades, grupos e perfis, gestão de métodos de MFA, gestão de aplicações web, gestão de senhas, gestão do portal dos usuários finais e autenticação de usuários finais utilizando os métodos de MFA oferecidos.

11. ENTREGAS PREVISTAS

Plataforma de Gestão de Acessos e Autenticação Centralizada integrada a PLATAFORMA SP, com capacidade para 285 mil servidores;

Infraestrutura Virtualizada on Premises (IaaS) Avançada com Serviço de Suporte Avançado;

Ferramenta de Monitoramento de Aplicações;

Serviço de Implantação, configuração e Implementação; e

Serviço de Manutenção, Suporte Técnico e Garantia

12. IMPLANTAÇÃO DO PROJETO

Após a assinatura do contrato deverá ser realizada em até 05 (cinco) dias úteis a reunião inicial com a CONTRATADA.

A Reunião Inicial tem como o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato e Termo de Referência, informar a previsão das necessidades e esclarecer possíveis dúvidas acerca da execução dos serviços.

A CONTRATATADA deverá cumprir os eventos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos, os quais poderão ser antecipados sempre que as circunstâncias assim o permitam. Os tempos considerados na tabela a seguir são contados em dias úteis.

Evento	Descrição do Evento	Prazo
1	Assinatura do contrato	-
2	Reunião Inicial	Até 05 (cinco) dias após a assinatura do contrato
3	Disponibilização da solução e início dos serviços	Até 10 (dez) dias após a emissão da Ordem de Serviço
4	Ativação da solução	Até 30 (trinta) dias após a disponibilização dos Serviços.

A CONTRATADA deverá informar e providenciar local de acesso e/ou ferramenta para gerenciamento, controle e suporte à implantação para as licenças de software utilizadas na execução do serviço.

13. MODELO DE EXECUÇÃO DO CONTRATO

A SGGD, por intermédio do Gestor do Contrato, convocará a CONTRATADA, imediatamente após a assinatura do contrato, para reunião de alinhamento de entendimentos e expectativas, ora denominada reunião inicial, com o objetivo de:
Alinhar a forma de comunicação entre as partes, que deverá ocorrer preferencialmente entre a SGGD e a CONTRATADA;
Definir as providências necessárias para inserção da CONTRATADA no ambiente de prestação dos serviços;
Definir as providências de implantação dos serviços;
Alinhar entendimento quanto aos modelos de execução e de gestão do contrato.

13.1. <u>Mecanismos formais de comunicação</u>

São definidos como mecanismos formais de comunicação, entre a SGGD e a CONTRATADA, os seguintes:
Ordem de Serviço;
Ata de Reunião;
Ofício;
Canal de abertura de chamados;
E-mails

A CONTRATADA deve comunicar a SGGD, por escrito e em tempo hábil, quaisquer anormalidades que impeçam a execução parcial ou total do objeto licitado, prestando todos os esclarecimentos necessários.

13.2. <u>Papéis e Responsabilidades</u>

São papéis desempenhados na gestão do contrato proveniente deste Termo de Referência.

Responsável/Função	**Atribuições**
Gestor do Contrato	Servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente. Atribuições Encaminhar a Ordem de Serviço e informar desvios de qualidade quando necessário; Monitorar a execução do contrato; e Autorizar a emissão/pagamento de notas fiscais.

Fiscal do contrato	Servidor da SGGD com conhecimentos de fiscalização de contratos de TI. Atribuições Monitorar e fiscalizar tecnicamente o contrato; Acompanhar a execução das Ordens de Serviço; Apoiar o Gestor do contrato quanto às questões técnicas contratuais; Acompanhar implantação da solução, atestar o funcionamento da solução, e, no caso de falhas ou dúvidas, acionar o suporte técnico contratado junto com a solução para garantir manutenção e operacionalidade.

14. CRITÉRIOS DE ACEITAÇÃO

A CONTRATANTE emitirá o termo de aceite para os serviços executados, após a constatação de sua implantação/realização considerando às especificações técnicas e os Níveis Mínimos de Serviço estabelecidos neste Termo de Referência.

O prazo máximo para emissão do Termo de Aceite do serviço é de 15 dias, a contar da data de implantação/realização do serviço. Caso o serviço apresente problemas ou não atendam às especificações técnicas, o prazo de aceite será reiniciado após a solução dos problemas detectados.

O prazo máximo para a CONTRATADA solucionar os problemas reportados é de 15 dias a contar do comunicado da CONTRATANTE.

15. SUPORTE TÉCNICO

Para as aberturas de chamados e respostas aos problemas e incidentes, a CONTRATADA deverá cumprir com os tempos a seguir:

Nível	Criticidade	Descrição	Tempo para Resposta e Solução a partir do acionamento
Severidade 1	Crítico	O uso do sistema é interrompido ou tão severamente afetado que não possibilita continuidade no trabalho. A perda do serviço é total. Trata-se de emergência, a operação é essencial para o negócio e produtividade futura. O ambiente apresenta pelo menos uma das seguintes situações: Dados corrompidos; Uma função crítica documentada não está disponível; O sistema trava indefinidamente, causando demoras inaceitáveis ou indefinidas para recursos ou respostas; O sistema falha repetidamente após tentativas de reinicialização. A SGGD alocará um contato durante este período, seja no local ou por telefone, para auxiliar na coleta de dados, testes e aplicação de correções.	04 horas – Horário comercial
Severidade 2	Importante	A perda do serviço é significativa, funcionalidades importantes não estão disponíveis, a operação continua de forma limitada e precária. A produção opera de acordo com as especificações sem que exista solução temporária para o problema ou ainda, a CONTRATANTE não consegue prosseguir com a instalação de qualquer produto contratado, impedindo-o de disponibilizá-lo aos usuários.	08 horas - Horário comercial
Severidade 3	Menor	A perda do serviço é pequena, o problema gera inconvenientes que	1 dia útil

		podem exigir uma solução alternativa para restaurar a funcionalidade	
Severidade 4	Leve	Não há impacto na operação e perda de serviço. O resultado não impede o funcionamento do sistema	02 dias úteis

A CONTRATADA pode apresentar uma solução de contorno para o restabelecimento da solução, até que possa apresentar a solução definitiva.

A CONTRATADA envidará esforços contínuos para solucionar as Solicitações de Serviços (SRs - Services Request) de Severidades 1 e 2.

A CONTRATADA iniciará escalonamento interno para os SRs de Severidade 1 e Severidade 2de acordo com as Respostas às Solicitações de Serviços.

A CONTRATADA priorizará o reparo de defeitos dos softwares utilizados nos serviços durante a resolução dos chamados.

16. NÍVEIS MÍNIMOS DE SERVIÇO

Para fins desta contratação considera-se Nível Mínimo de Serviços – NMS, a definição em termos tangíveis e objetivamente observáveis, dos níveis esperados de qualidade de prestação de serviço e as respectivas adequações de pagamento.

NMS	Incide sobre	Nível Mínimo de Serviço (NMS)	Fórmula para Determinação do Impacto por não cumprimento do NMS	Penalidade
Atraso no prazo de implantação da solução	Valor da OS	Cumprir o prazo de entrega constante na OS	Dias úteis de atraso na entrega do Serviço	1% (um por cento) para cada dia útil de atraso na entrega, limitado a 10% (dez por cento) do valor da OS
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Crítico)	Valor unitário do Serviço	Prazo de solução em até 4 (quatro) horas - horário comercial	Números de horas de atraso para solução do chamado	0,2% (dois décimos por cento) por hora de indisponibilidade, limitado a 5% (cinco por cento) do valor do serviço
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Importante)	Valor unitário do Serviço	Prazo de solução em até 8 (oito) - horário comercial	Números de horas de atraso para solução do chamado	0,2% (dois décimos por cento) por hora de indisponibilidade, limitado a 2% (dois por cento) do valor do serviço
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Menor)	Valor unitário do Serviço	Prazo de solução em até 1 (um) – dia útil	Números de horas de atraso para solução do chamado	0,1% (um décimo por cento) por hora de indisponibilidade, limitado a 2% (dois por cento) do valor do serviço
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Leve)	Valor unitário do Serviço	Prazo de solução em até 2 (dois) – dias úteis	Números de horas de atraso para solução do chamado	0,1% (um décimo por cento) por hora de indisponibilidade, limitado a 1% (um por cento) do valor do serviço

17. FORMA DE CONTRATAÇÃO

A contratação do objeto pretendido se refere a bens e serviços comuns, sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante contratação direta, com fundamento na GN 2349-15.

A contratação da Prodesp além de possuir o respaldo legal, porquanto prevista no Contrato de Empréstimo BID 5579/OC-BR (BR-L1591), tem respaldo técnico, visto que ela é responsável pela sustentação técnica do INTEGRADORSP, IDPSP, bem como é responsável pelo desenvolvimento do PLATAFORMASP. Além do mais a Prodesp possui experiência na implantação de solução de gestão de identidades e acessos.

Por fim é importante ressaltar que a contratação da Prodesp está em consonância com a Estratégia de Governo Digital instituída pelo Decreto nº 67.799/2023, que no art. 7º e parágrafo único, que assim estabelece:

“Artigo 7° - A Companhia de Processamento de Dados do Estado de São Paulo - PRODESP tem por atribuição prestar, na forma de seu estatuto social, os serviços de tecnologia da informação e comunicação necessários ao Sistema Estadual de Tecnologia da Informação - SETIC, de que trata o Decreto n° 64.601, de 22 de novembro de 2019, e à execução da Estratégia de Governo Digital e dos Planos Diretores de Tecnologia da Informação e Comunicação previstos neste decreto.

Parágrafo único - Cabe aos órgãos e entidades priorizar a contratação da PRODESP para prestação dos serviços de que trata o "caput" deste artigo, observadas as normas legais e regulamentares aplicáveis à espécie.”

18. ESTIMATIVA DE CUSTO DA CONTRATAÇÃO

A estimativa do custo total da contratação foi elaborada com base no datalhamento do escopo realizado entre a equipe técnica da SGGD e equipes técnicas e comercias da Prodesp. O valor estimado para a pretensa contratação é de R$110.000.000,00 (Cento de dez milhões de reais).

19. CONDIÇÕES COMERCIAIS E DE PAGAMENTO

O pagamento do licenciamento referente a Plataforma de Gestão de Acessos e Autenticação Centralizada ocorrerá na modalidade “up-front”, a partir da ativação das licenças e disponibilização da plataforma, após emissão da nota fiscal/fatura e após a devida atestação pela SGGD.

O pagamento dos serviços relacionados a implantação e ativação do suporte ocorrerá em parcela única, após emissão da nota fiscal/fatura e após a devida atestação pela SGGD.

O pagamento dos serviços relacionados ao suporte da solução, monitoramento e serviços técnicos ocorrerá mensalmente, após emissão da nota fiscal/fatura e após a devida atestação pela SGGD.

20. VIGÊNCIA

A contratação terá vigência de 24 (vinte e quatro) meses contados a partir da data da sua assinatura, podendo ser prorrogado por períodos e sucessivos durante a vigência do contrato de empréstimo (5579/OC-BR).

ANEXO II – ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS Nº E0240240

Este documento, a partir de sua assinatura, fará parte integrante do Contrato de Prestação de Serviços PD024142, firmado com a Secretaria de Gestão e Governo Digital - SGGD.

1. OBJETO

Disponibilização de uma Plataforma como Serviço – PaaS Middleware para uma Solução de Gerenciamento de Identidades e Acessos

2. ESCOPO DA PRESTAÇÃO DE SERVIÇOS

2.1. CONTEXTO

Alinhado aos princípios e objetivos da Estratégia de Governo Digital, decreto 67.799 de 13 de julho de 2023, e com o objetivo de melhorar a eficiência e a transparência da gestão pública, a SGGD irá desenvolver a Plataforma SP que tem como objetivo centralizar as atividades executadas pelos servidores públicos relacionadas a disponibilização dos serviços digitais do estado de São Paulo.

A plataforma SP é baseada em dois pilares tecnológicos, a disponibilização de uma plataforma com interface customizada que permita a interoperabilidade com outros sistemas do governo do estado, através de API (Application Programming Interface) e uma solução de gerenciamento de identidades e acessos que é o enfoque desta proposta.

Essa abordagem oferece camadas adicionais de proteção aos fluxos de trabalho críticos, permitindo a detecção de comportamentos suspeitos, simplificando a autenticação e a auditoria detalhada e reduzindo a exposição de credenciais, minimizando os riscos de segurança e vazamento de dados. Almeja-se, assim, a redução de incidentes de fraude e a promoção de uma cultura de segurança da informação entre os colaboradores.

2.2. ATIVIDADES PREVISTAS

Faz parte do escopo desse serviço:

• PaaS Middleware para 285 mil servidores com Serviço de Gestão de Middleware Avançado

• Infraestrutura Virtualizada on Premises (IaaS) Avançada com Serviço de Suporte Avançado

• Ferramenta de Monitoramento de Aplicações

• Serviço de Implantação, configuração e Implementação

• Serviço de Manutenção, Suporte Técnico e Garantia

2.2.1. Plataforma PaaS Middleware

Este serviço disponibilizará todo o licenciamento necessário para a Solução de Gerenciamento de Identidades e Acessos, garantindo o correto funcionamento da plataforma, bem como a troca de dados de forma segura entre seus diversos módulos, além de disponibilizar em um único local a autenticação, autorização e segurança das identidades para aplicações e servidores públicos com Serviço de Gestão de Middleware Avançado.

O PaaS Middleware está previsto para suportar 285.000 (duzentos e oitenta e cinco mil) servidores públicos que no desempenho das suas atividades utilizam diretamente a Plataforma SP ou um dos sistemas governamentais que vão interoperabilizar com a plataforma.

A proposta da plataforma disponibilizada na modalidade SaaS (Service as a Service) contemplará:

• Serviço de gestão de acessos com portal Single Sign-On (SSO) e Autenticação Multifator (MFA), por meio de um catálogo de aplicações web com modelos de configuração de SSO abrangendo as aplicações mais conhecidas do mercado como SAML 2.0; Oauth 2.0 modo cliente, WS-Federation, OpenID connect, NTLM, Oauth 2.0 modo server e HTTP Basic.

• Tecnologia com algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados para cálculo de risco;

• Medição do risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos: Geo Velocidade (velocidade do deslocamento do login, traçando comportamento do usuário), Geo Localização (verificação da localização geográfica do acesso atual em comparação com o seu comportamento usual), Dia da Semana (dia da semana do acesso atual em comparação com seu comportamento usual), Horário de Acesso (horário do acesso atual em comparação com seu comportamento usual), Sistema Operacional (Sistema Operacional do acesso atual em comparação com seu comportamento usual) e Falhas de Login Consecutivas (falhas de login consecutivas do acesso atual em comparação com seu comportamento usual);

• Disponibilização de múltiplo fator de autenticação para casos de uso com capacidade de interpretação de risco adaptativo baseados em algoritmos de aprendizado de máquina e reconhecimento de comportamentos temporais para cada identidade (dias da semana e horários), o mesmo calculado antes da autenticação, visando a tomada de ações antes da materialização da autenticação;

• Disponibilização de personalização das faixas de pontuação (0 a 100) para os administradores para, no mínimo, as categorias: sem risco, baixo, médio e alto risco;

• Serviço de acesso seguro sem VPN para aplicações web hospedadas on premises;

• Tecnologia embarcada para intermediar o SSO em aplicações web sitiadas no datacenter da PRODESP ou de seus clientes sem a necessidade de expor estas aplicações para a internet ou uso de VPN, suportando os mesmos métodos e protocolos do item anterior;

• Nuvem para intermediar o fluxo de dados entre a aplicação sitiada no datacenter da PRODESP ou de seus clientes e o navegador personalizado e configurado que acessa a aplicação, com a finalidade de não expor diretamente o acesso;

• Importação de certificados digitais para prover personalização do domínio acessado via nuvem;

• Bloqueio de acesso a aplicação com o IP inicial da conexão, caso haja alteração, com solicitação de re-autenticação ao usuário;

• Opção de respeitar ou não o tempo de expiração do cookie de autenticação gerado na autenticação pela nuvem disponibilizada e não da aplicação;

• Reescrever a URL externa com a URL interna da aplicação;

• Capacidade de fail over e load balance nativamente sem a necessidade de balanceadores de carga;

• Serviço de orquestração do aprovisionamento de identidades;

• Criação e disponibilização de um catálogo com templates de integração com pelo menos 5.000 (cinco mil) exemplos;

• Provisionamento de identidades usando os protocolos modernos REST ou SCIM; o Provimento não somente da capacidade de autenticação, mas também o aprovisionamento /deprovisionamento de identidades em aplicações SaaS, contemplando, no mínimo, o aprovisionamento com modelos prontos no catálogo para: Office 365, Google Workspaces, Azure, Amazon Web Services, Docusign, Salesforce, ServiceNow, Zendesk;

• REST API para as seguintes operações:

▪ Operações de criação, leitura, atualização e deleção em objetos do tipo usuário.

▪ Operações de criação, leitura, atualização e deleção em objetos do tipo grupo.

• Aprovisionamento em aplicações que suportem interfaces gerenciamento de identidades entre domínios (SCIM), padrão de mercado para aplicações entregues no modelo SaaS para aprovisionamento de identidades;

• Provisionamento com base nas funções (perfis) já configuradas;

• Capacidade de reconhecimento de alterações em grupos do Active Directory e com base nessas alterações, realizar o provisionamento automaticamente em funções nas aplicações conectadas;

• Capacidade de transformar dados e atributos para atender aos requisitos de negócios e fornecer os dados necessários nas aplicações conectadas;

• Oferta aos usuários da capacidade de solicitar acessos para aplicativos com fluxos de aprovação configuráveis;

• Capacidade de desprovisionar as identidades nos aplicativos automaticamente com base nas mudanças nas funções ou na desativação de uma conta de usuário com a opção de excluir ou desativar a identidade no aplicativo conectado;

• Sincronismo completo ou incremental das identidades e permissões nas aplicações conectadas, com capacidade de fornecer relatórios completos sobre estes sincronismos com as falhas e modificações ocorridas. Estes serão acessíveis por interface web e também envio automático por e-mail na finalização de um ciclo de sincronismo;

• Serviço de orquestração de requisições aprovações e aprovisionamento por workflows;

• Criação e disponibilização de um módulo de criação de workflows no estilo no-code, ou seja, sem a necessidade de nenhum tipo de codificação utilizando somente parametrizações, para integração e automação do fluxo de informação de identidades, assim facilitando a integração com sistemas de ITSM, provisionamento de identidades em aplicações, tomadas de decisão, transformação e agregação de dados;

• Capacidade de criação de formulários de entradas de dados totalmente personalizáveis, sem necessidade de codificação. Os formulários podem ser utilizados em qualquer parte do fluxo de trabalho visando melhorar a tomada de decisão e fornecimento de mais informações de forma manual durante a execução de um workflow;

• Oferta de uma biblioteca com chamadas de APIs préconfiguradas para as principais soluções de mercado, citando como exemplo, AWS, Azure, GCP, ServiceNow, Slack, soluções de Recursos Humanos dentre outros.

• Realização da importação de APIs que não estão presentes no catálogo através do formato OpenAPI - padrão de mercado;

• Criação de workflows WEB;

• Serviço de workflow como um gateway SCIM (System for Cross Domain Identity Management), padrão de mercado para gestão de identidades entre aplicações. Capacidade de receber chamadas do tipo SCIM e converter em chamadas web API para aplicações que não suportem chamadas SCIM nativamente, funcionando como um tradutor de qualquer chamada SCIM para web APIs e vice-versa;

• Banco de dados interno com acesso via Workflows para persistência e consulta de dados dos wokflows em execução;

2.2.1.1. Entregáveis

• Relatórios de justificativas e aprovações internas;

• Controles de vigência dos licenciamentos;

• Renovações e disponibilidade do licenciamento contratado junto ao fornecedor;

• Controles e medições das licenças disponibilizadas no portal do fornecedor;

• Habilitação / ativação das licenças e envio de informação ao cliente (serial, chave de instalação);

• Orientação e apoio técnico quanto a ativação local e instalação;

• Orientação técnica remota ou presencial, quando necessário;

• Apoio técnico na gestão de usuários e atribuição de licenciamento;

• Apoio técnico no tratamento de incidentes / Troubleshooting;

• Construção e gerenciamento de grupos de usuários para controle de acessos;

• Métricas de uso;

2.2.2. Infraestrutura Virtualizada On Premises (IaaS) Avançada com Serviço de Suporte Avançado para Gateway de Aplicação Web

Fornecimento de capacidade de processamento, memória, armazenamento de dados e sistema operacional com proteção antivírus, para sistemas críticos com toda a segurança do Data Center Prodesp (certificações ISO 9001, 27001, 20000 e 14001), por meio da:

• Criação dinâmica de servidores virtuais;

• Realocação de servidores lógicos, sem interrupção dos serviços;

• Recuperação automática em caso de falha do hardware;

• Licenças de Sistemas Operacionais e Antivírus homologados pela CONTRATADA

• Instalação do Sistema Operacional dos servidores;

• Instalação de Antivírus em servidores, incluindo atualizações da biblioteca de vírus;

• Instalação de agente de Backup;

• Backup e Restore - Administração das rotinas de backup / Restore com retenção de dados de 30 (trinta) dias (21 (vinte e um) dias para Banco de Dados), conforme o ANEXO A - Formulário da Ficha de Backup e as políticas de backup da CONTRATADA.

• Power-on (ligação) da máquina virtual, garantindo a disponibilidade;

2.2.2.1. Entregável

Gerenciamento do ambiente, sendo responsável pela disponibilidade das aplicações e sistema operacional hospedado na máquina virtual, incluindo os serviços de administração das máquinas virtuais (solicitar criação, configuração, desligamento), administração de usuários (criação, remoção), controle de consumo, monitoramento, gerenciamento e suporte técnico para os servidores virtuais e camadas de aplicação, exibição e banco de dados. Principais atividades:

• Administração VNET, sbnets, tabela de roteamento;

• Configuração das soluções de segurança utilizando os recursos VPN, WAFs, NSGs, Anti-DDoS, Security Endpoint e Firewalls disponíveis;

• Gerenciamento de segurança centralizado dos recursos de rede;

• Monitoramento e identificação de ataques no ambiente que possuam as soluções de VPN, WAF (web application firewall) Firewall e Anti-DDoS utilizando Log Analytic workspace;

• Acompanhamento operacional das ferramentas disponibilizadas para o monitoramento do ambiente;

• Aplicação de soluções de contorno baseado em scripts pré-definidos minimizando impacto nos negócios;

• Provisionamento e Desprovisionamento de recursos de infraestrutura;

• Administração e Configuração das máquinas virtuais;

• Atuação em caso de recomendações de performance

2.2.3. Ferramenta de Monitoramento de Aplicações

Inclui as funcionalidades relativas às ferramentas de monitoramento da infraestrutura, tais como, indicadores de utilização de processamento, memória, disco e as respostas das portas do servidor, de forma a auxiliar no acompanhamento da saúde do ambiente (produção/homologação);

A solução auxilia na identificação da causa raiz de problemas de desempenho, por meio do monitoramento profundo da aplicação, em seus diversos aspectos, tais como: URLs, classes, métodos, erros, exceções, queries, dump de memória, entre outros, além de identificar a origem de problemas de desempenho ou disponibilidade, medindo tanto o tempo de execução, como também os tempos de sincronização, I/O, CPU, garbage collection, entre outros;

Entregáveis:

• Disponibilização de console administrativo com opção de emitir relatórios sobre os incidentes gerados;

• Envio de alertas notificando sobre a ocorrência de problemas ou eventos pré-definidos;

• Criação de dashboards (painéis), com visões consolidadas das métricas de desempenho de infraestrutura, operacionais e de negócio;

• Confirmação das informações dos eventos, incidentes e alarmes gerados automaticamente pela plataforma de monitoramento;

• Notificação das áreas técnicas da CONTRATANTE para atuação na solução dos problemas identificados quando necessário;

• Acionamento de fornecedores de serviços para reparos em software, link e equipamento;

• Realização da gestão dos incidentes e escalonamentos necessários;

• Acompanhamento da execução/encerramento dos chamados;

• Comunicado informativo às áreas competentes sobre eventuais indisponibilidades dos serviços.

2.2.4. Serviço de Implantação, configuração e Implementação

• Mobilização das equipes;

• Elaboração dos termos de início e encerramento do projeto;

• Elaboração de cronograma de atividades em conjunto com a SGGD;

• Organização de reuniões e interação com as partes interessadas;

• Relatório periódico de status;

• Monitoramento e controle do projeto quanto à sua evolução, tratando eventuais mudanças;

• Elaboração de termos de aceite para formalização de entregas;

• Fornecimento de todo o apoio técnico e gerencial necessário para o início do projeto, compreendendo atividades especializadas de implementação e customização de políticas conectores e alertas;

• Disponibilização e configuração do serviço de integração de aplicações nativas do tipo SAML e/ou OpenID;

• Emissão de relatórios técnicos e gerenciais relacionados à implementação do projeto, como relatório de status report, relatórios de riscos e problemas e relatório de conclusão do projeto;

• Ativação inicial do licenciamento relacionado às soluções contratadas;

• Instalação e parametrização dos componentes;

• Configuração inicial de conectores, políticas e alertas.

2.2.5. Serviço de Manutenção, Suporte Técnico e Garantia

• Administração centralizada, permitindo acesso à console para gestão e monitoramento eficaz de identidades, papéis e aplicações;

• Auxílio na configuração de políticas de autenticação, garantindo a segurança contínua das suas identidades;

• Suporte à configuração de aplicações e políticas de acesso;

• Auxílio para configuração de integrações de aplicações nativas do tipo SAML e/ou OpenID.

• Auxílio para configuração de aplicações genéricas ou com acesso via usuário e senha. • Auxílio para configuração de fluxos de automação;

• Auxílio na configuração de provisionamentos de Identidades usando SCIM ou integrações nativas;

• Apoio na configuração de políticas personalizadas para atender às necessidades específicas da SGGD.

• Desenvolvimento de Relatórios:

  • Relatórios técnicos e gerenciais contemplando a auditoria de alterações de políticas, estatística de usuários com fatores de risco e acessos a aplicações para fornecimento de insights sobre a segurança das identidades.

• Manutenção Preventiva e Corretiva:

  • Fornecimento de atualizações regulares do software conforme disponibilização de novas versões do fabricante para garantir a segurança e o desempenho otimizado do sistema. Resolução de problemas emergentes por meio de correções de bugs e patches de segurança. Revisões periódicas de desempenho e integridade do sistema para identificar e resolver possíveis problemas antes que afetem a operação.

• Suporte Técnico Especializado:

  • Disponibilização de equipe de suporte técnico dedicada e altamente qualificada, disponível para resposta a consultas e resolução de problemas técnicos de forma rápida e eficiente;

  • Utilização de ferramenta de ITSM para abertura de chamados garantindo uma resposta rápida e eficaz às necessidades;

  • Suporte remoto para diagnóstico de problemas e solução de questões técnicas sem a necessidade de intervenção presencial, garantindo uma resolução mais ágil dos problemas.

2.2.5.1. Entregáveis

Disponibilização de dashboards pré-configurados com informações e gráficos com as seguintes características:

• Utilização do Motor de Análise do Comportamento dos Usuários;

• Visão sobre a segurança das aplicações;

• Mapa com a geolocalização das autenticações;

• Visão sobre o comportamento dos endpoints (mobile e computadores);

• Visão sobre o comportamento das identidades;

Disponibilização de dashboards personalizados, e possibilidade de compartilhamento dos dashboards com outros usuários; Identificação dos atributos de contexto de cada autenticação, contendo minimamente:

• Endereçamento IP;

• Dia da Semana;

• Datas específicas;,

• Janelas de tempo entre duas datas;

• Janelas de tempo entre horários (por exemplo: horário comercial);

• Tipo do Sistema Operacional;

• Tipo do Browser;

• Perfis configurados;

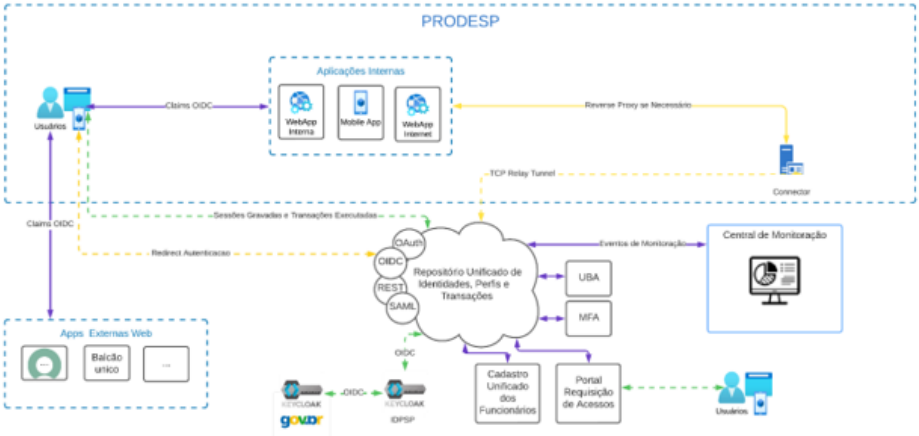
• País que está sendo realizado o acesso;

• Se é um dispositivo gerenciado;

• Autenticação via certificado;

• Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários.

2.3. TOPOLOGIA DA SOLUÇÃO



2.4. SUPORTE TÉCNICO

Disponibilização de equipe de suporte técnico para responder a consultas e resolver problemas técnicos de forma rápida e eficiente, por meio da utilização de ferramenta de ITSM para abertura de chamados suporte remoto para diagnóstico de problemas e solução de questões técnicas sem a necessidade de intervenção presencial. Para as aberturas de chamados e respostas aos problemas e incidentes:

Nível	Criticidade	Descrição	Tempo para Resposta e Solução a partir do acionamento
Severidade 1	Crítico	O uso do sistema é interrompido ou tão severamente afetado que não possibilita continuidade no trabalho. A perda do serviço é total. Trata-se de emergência, a operação é essencial para o negócio e produtividade futura. O ambiente apresenta pelo menos uma das seguintes situações: Dados corrompidos; Uma função crítica documentada não está disponível; O sistema trava indefinidamente, causando demoras inaceitáveis ou indefinidas para recursos ou respostas; O sistema falha repetidamente após tentativas de reinicialização. A **SGGD deverá alocar** um contato durante este período, seja no local ou por telefone, para auxiliar na coleta de dados, testes e aplicação de correções.	04 horas – Horário comercial
Severidade 2	Importante	A perda do serviço é significativa, funcionalidades importantes não estão disponíveis, a operação continua deforma limitada e precária. A produção opera de acordo com as especificações sem que exista solução temporária para o problema ou ainda, a PRODESP não consegue prosseguir com a instalação de qualquer produto contratado, impedindo-o de disponibilizá-lo aos usuários.	08 horas - Horário comercial
Severidade 3	Menor	A perda do serviço é pequena, o problema gera inconvenientes que podem exigir uma solução alternativa para restaurar a funcionalidade	2 dias úteis
Severidade 4	Leve	Não há impacto na operação e perda de serviço. O resultado não impede o funcionamento do sistema	04 dias úteis

2.5. NÍVEIS MÍNIMOS DE SERVIÇO

Para fins desta ESP considera-se Nível Mínimo de Serviços – NMS, a definição em termos tangíveis e objetivamente observáveis, dos níveis esperados de qualidade de prestação de serviço e as respectivas adequações de pagamento:

NMS	Incide sobre	Nível Mínimo de Serviço (NMS)	Fórmula para Determinação do Impacto por não cumprimento do NMS	Penalidade
Atraso no prazo de implantação do Serviço	Valor da OS	Cumprir o prazo de entrega constante na OS	Dias úteis de atraso na entrega do Serviço	1% (um por cento) para cada dia útil de atraso na entrega, limitado a 10% (dez por cento) do valor da OS
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Crítico)	Valor unitário do Serviço	Prazo de solução em até 4 (quatro) - horário comercial	Números de horas de atraso para solução do chamado	0,2% (dois décimos por cento) por hora de indisponibilidade, limitado a 5% (cinco por cento) do valor do serviço
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Importante)	Valor unitário do Serviço	Prazo de solução em até 8 (oito) - horário comercial	Números de horas de atraso para solução do chamado	0,2% (dois décimos por cento) por hora de indisponibilidade, limitado a 2% (dois por cento) do valor do serviço
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Menor)	Valor unitário do Serviço	Prazo de solução em até 2 (dois) – dias úteis	Números de horas de atraso para solução do chamado	0,1% (um décimo por cento) por hora de indisponibilidade, limitado a 2% (dois por cento) do valor do serviço
Atraso na Solução a partir do acionamento do chamado de Severidade 1(Leve)	Valor unitário do Serviço	Prazo de solução em até 4 (quatro) – dias úteis	Números de horas de atraso para solução do chamado	0,1% (um décimo por cento) por hora de indisponibilidade, limitado a 1% (um por cento) do valor do serviço

3. PRAZOS

O cronograma para execução dos trabalhos previstos nesta ESP será estabelecido de comum acordo entre as partes.

4. RESPONSABILIDADE DAS PARTES

Além das obrigações constantes da Cláusula “OBRIGAÇÕES DAS PARTES” do Contrato a que se vincula esta ESP ficam definidas as enunciadas a seguir:

4.1. DA CONTRATADA

4.1.1. Designar as pessoas responsáveis que serão os interlocutores autorizados para o relacionamento com a CONTRATANTE;

4.1.2. Participar, juntamente com pessoal da CONTRATANTE de reuniões periódicas de acompanhamento e avaliação das atividades previstas nesta ESP;

4.1.3. Comunicar imediatamente, todas as ocorrências imprevistas que prejudiquem a prestação de serviços;

4.2. DA CONTRATANTE

4.2.1. Designar as pessoas responsáveis que serão os interlocutores autorizados para o relacionamento com a CONTRATADA;

4.2.2. Designar as pessoas responsáveis pela comunicação com a CONTRATADA;

4.2.3. Fornecimento de materiais (equipamentos, peças e licenças) eventualmente necessários à execução dos serviços.

5. PREÇO E CONDIÇÕES DE PAGAMENTO

O preço para a execução dos serviços constantes desta ESP é estimado em **R$ 113.915.008,41 (cento e treze milhões, novecentos e quinze mil, oito reais e quarenta e um centavos)**, tendo como data base de referência o mês de **novembro/2024** e será reajustado de acordo com as condições estabelecidas no contrato a que se vincula.

	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	VALOR UNITÁRIO	QTDE PREVISTA MENSAL	QTDE DIAS	VALOR ESTIMADO MENSAL	PARCELA ÚNICA	QTD MESES	Desconto Incondicional	TOTAL ESTIMADO
5.1	**PLATAFORMA COMO SERVIÇO (PaaS) PARA DISPONIBILIZAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E ACESSOS**					**115.676,31**	**109.123.447,66**			**107.795.742,93**
5.1.1	MIDDLEWARE - PARCELA ÚNICA	UNIDADE DE MIDDLEWARE	1.691,08	64.528,85			109.123.447,66	1	4.193.984,17	104.929.463,49
5.1.2	MIDDLEWARE - PARCELA MENSAL	UNIDADE DE MIDDLEWARE	1.691,08	62,99		106.521,13		24		2.556.507,12
5.1.3	SERVIÇOS DE GESTÃO DE MIDDLEWARE - AVANÇADO	POR UNIDADE DE GESTÃO / MÊS	9.157,18	1		9.157,18		24		219.772,32
5.2	**INFRAESTRUTURA VIRTUALIZADA ON PREMISES AVANÇADO COM SERVIÇOS DE SUPORTE AVANÇADO - GATEWAY APLICAÇÕES WEB**					**25.192,98**	**400,59**			**605.032,11**
5.2.1	MÁQUINA VIRTUAL CATEGORIA III	SERVIDOR/MÊS	1.967,57	9		17.708,13		24		424.995,12
5.2.2	RECURSOS ADICIONAIS - MEMÓRIA	GRAMMÊS	56,41	72		4.061,52		24		97.476,48
5.2.3	SERVIÇO DE SUPORTE AVANÇADO	POR SERVIDOR / MÊS	380,37	9		3.423,33		24		82.159,92
5.2.4	ATIVAÇÃO DE SERVIÇO DE SUPORTE AVANÇADO	POR SERVIDOR	44,51	9			400,59	1		400,59
5.3	**FERRAMENTA DE MONITORAMENTO DE APLICAÇÕES**					**14.396,40**	**305,19**			**345.818,79**
5.3.1	MONITORAMENTO DE APLICAÇÕES - SERVIDOR COM ATÉ 16 GB RAM	POR SERVIDOR / DIA	53,32	9	30	14.396,40		24		345.513,60
5.3.2	SERVIÇO DE ATIVAÇÃO - ATIVAÇÃO DE ATÉ 10 SERVIDORES	ATIVAÇÃO ATÉ 10 SERVIDORES	305,19	1			305,19	1		305,19
5.4	**SERVIÇOS DE INSTALAÇÃO - SERVIDOR HTTP**	**POR SERVIDOR**	**925,76**	**9**			**8.332,02**	**1**		**8.332,02**
5.5	**Serviços Técnicos Especializados - ANALISTA DE SUPORTE Nível 2 (Hora Comercial - 08h de 2ª à 6ª das 06:00 às 22:00)**	**HORA HOMEM**	**104,10**	**60**		**6.246,00**		**24**		**149.904,00**
5.6	**Serviços de Manutenção, Suporte Técnico e Garantia**	**UNIDADE**	**212.507,44**	**1**		**212.507,44**		**24**		**5.100.178,56**
	TOTAL					**374.021,13**	**104.938.501,29**			**113.915.008,41**

Os serviços serão faturados a partir da disponibilização da Plataforma de PaaS Middleware para Solução de Gerenciamento de Identidades e Acessos, conforme abaixo:

• O subitem 5.1.1 será faturado em parcela única após 90 (noventa) dias da emissão da OS – Ordem de Serviço. Para este item, será concedido desconto comercial incondicional de R$4.193.984,17;

• Os subitens 5.1.2, 5.1.3, 5.6 em parcela fixa mensal;

• Os subitens 5.2.1, 5.2.2, 5.2.3, 5.3.1 e 5.5, mensalmente de acordo com as quantidades apuradas no final de cada mês;

• Os subitens 5.2.4, 5.3.2 e 5.4 em parcela única após a instalação.

Serão emitidas Notas Fiscais Eletrônicas e enviadas, automaticamente, pelo sistema das Prefeituras (Taboão da Serra e São Paulo), sendo que para os serviços prestados em Taboão da Serra, serão encaminhadas para o e-mail cadastrado no sistema de contratos da Prodesp, e para os serviços prestados em São Paulo, para o e-mail cadastrado junto àquela Prefeitura.

Recebidas as Notas-Fiscais Eletrônicas, a CONTRATANTE terá o prazo de 03 (três) dias úteis para atestação da execução dos serviços ou devolução para esclarecimentos e correções necessárias.

Os pagamentos deverão ser efetuados dentro do prazo de 30 (trinta) dias da data de apresentação das Notas-Fiscais Eletrônicas.

DO DESCONTO COMERCIAL INCONDICIONAL:

A Prodesp, como empresa pública e parceira estratégica da administração estadual, possui compromisso com a modernização e a melhoria dos serviços digitais oferecidos ao cidadão paulista e aos órgãos governamentais. A proposta para a Secretaria de Gestão e Governo Digital, que inclui o projeto SP+Digital, representa uma oportunidade única para a Prodesp consolidar seu papel como protagonista na transformação digital do Estado.

1. Relevância Estratégica do Projeto SP+Digital

O projeto SP+Digital será um marco na trajetória de transformação digital do Estado de São Paulo, integrando e ampliando os canais de atendimento e serviços digitais disponíveis aos cidadãos. Essa iniciativa coloca a Prodesp numa posição de destaque, sendo uma catalisadora da digitalização dos serviços públicos, elevando o patamar de atendimento e otimizando processos em benefício de toda a administração pública. O sucesso do SP+Digital fortalecerá o papel da Prodesp como referência em soluções tecnológicas para o governo.

2. Fortalecimento do Relacionamento com o Cliente e Alinhamento com os

Objetivos de Governo

Oferecer o desconto comercial proposto é uma estratégia de fortalecimento de longo prazo do relacionamento da Prodesp com a Secretaria de Gestão e Governo Digital, o que é fundamental para assegurar o sucesso do projeto e a continuidade das parcerias futuras. Esse relacionamento é crucial para que a Prodesp possa contribuir de maneira mais integrada e responsiva aos objetivos da Secretaria e demais órgãos governamentais. O desconto demonstra o comprometimento da Prodesp em investir no sucesso do projeto, compartilhando parte dos custos e contribuindo diretamente para o alcance dos objetivos governamentais de digitalização e acessibilidade.

3. Investimento no Posicionamento da Prodesp como Provedora de Inovação e Soluções de Tecnologia para o Governo

A concessão do desconto se justifica também pelo impacto que o projeto SP+Digital terá no posicionamento estratégico da Prodesp frente ao governo e ao mercado. Com um projeto de tal relevância, a Prodesp fortalecerá sua imagem como referência em tecnologia e inovação pública, o que pode abrir novas oportunidades de negócios, tanto dentro do setor público como em parcerias interinstitucionais e projetos de cooperação.

4. Comprometimento com Resultados e Garantia de Qualidade

Ao viabilizar economicamente o projeto através do desconto comercial, a Prodesp está alinhada com o propósito de garantir a entrega de alta qualidade, com prazos e objetivos bem definidos, assegurando que os órgãos governamentais possam usufruir dos benefícios do projeto de forma mais acessível.

Conclusão

Assim, a Prodesp acredita que a concessão do desconto comercial à Secretaria de Gestão e Governo Digital é uma medida estratégica e fundamentada no compromisso com a transformação digital do Estado, no fortalecimento das parcerias de longo prazo e no avanço da Prodesp como líder em inovação e prestação de serviços de tecnologia para o setor público.

6. VIGÊNCIA DO DOCUMENTO

A ESP terá vigência de 24 (vinte e quatro) meses a partir da data da assinatura do Contrato.

7. VALIDADE DOS PREÇOS

Os preços constantes desta ESP são válidos por 120 (cento e vinte) dias após a data de sua emissão.

8. CONTATO NA PRODESP

Os contatos relativos ao objeto constante desta ESP deverão ser feitos com:

9. ÁREA DE NEGÓCIOS

Nome : Selma Berezutchi Aftim

Endereço : Rua Agueda Gonçalves, 240 - Taboão da Serra - SP

Telefone : (11) 2868-3124

E-mail : deboramoraes@sp.gov.br

10. ÁREA RESPONSÁVEL PELA EXECUÇÃO DO SERVIÇO

Nome : Jobson Nunes de Souza

Endereço: Rua Agueda Gonçalves, 240 - Taboão da Serra - SP

Telefone : 2845-6947

E-mail : jobson.souza@sp.gov.br

Emissão: 07/11/2024

ANEXO III – PLANILHA DE ORÇAMENTO - ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS E0240240

	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	VALOR UNITÁRIO	QTDE PREVISTA MENSAL	QTDE DIAS	VALOR ESTIMADO MENSAL	PARCELA ÚNICA	QTD MESES	Desconto Incondicional	TOTAL ESTIMADO
5.1	**PLATAFORMA COMO SERVIÇO (PaaS) PARA DISPONIBILIZAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E ACESSOS**					**115.676,31**	**109.123.447,66**			**107.705.742,93**
5.1.1	MIDDLEWARE - PARCELA ÚNICA	UNIDADE DE MIDDLEWARE	1.691,08	64.528,85			109.123.447,66	1	4.193.984,17	104.929.463,49
5.1.2	MIDDLEWARE - PARCELA MENSAL	UNIDADE DE MIDDLEWARE	1.691,08	62,99		106.521,13		24		2.556.507,12
5.1.3	SERVIÇOS DE GESTÃO DE MIDDLEWARE - AVANÇADO	POR UNIDADE DE GESTÃO / MÊS	9.157,18	1		9.157,18		24		219.772,32
5.2	**INFRAESTRUTURA VIRTUALIZADA ON PREMISES AVANÇADO COM SERVIÇOS DE SUPORTE AVANÇADO - GATEWAY APLICAÇÕES WEB**					**25.192,90**	**400,59**			**605.032,11**
5.2.1	MÁQUINA VIRTUAL CATEGORIA III	SERVIDOR/MÊS	1.967,57	9		17.708,13		24		424.995,12
5.2.2	RECURSOS ADICIONAIS - MEMÓRIA	GRAM/MÊS	56,41	72		4.061,52		24		97.476,48
5.2.3	SERVIÇO DE SUPORTE AVANÇADO	POR SERVIDOR / MÊS	380,37	9		3.423,33		24		82.159,92
5.2.4	ATIVAÇÃO DE SERVIÇO DE SUPORTE AVANÇADO	POR SERVIDOR	44,51	9			400,59	1		400,59
5.3	**FERRAMENTA DE MONITORAMENTO DE APLICAÇÕES**					**14.396,40**	**305,19**			**345.818,79**
5.3.1	MONITORAMENTO DE APLICAÇÕES - SERVIDOR COM ATÉ 16 GB RAM	POR SERVIDOR / DIA	53,32	9	30	14.396,40		24		345.513,60
5.3.2	SERVIÇO DE ATIVAÇÃO - ATIVAÇÃO DE ATÉ 10 SERVIDORES	ATIVAÇÃO ATÉ 10 SERVIDORES	305,19	1			305,19	1		305,19
5.4	**SERVIÇOS DE INSTALAÇÃO - SERVIDOR HTTP**	**POR SERVIDOR**	**925,78**	**9**			**8.332,02**	**1**		**8.332,02**
5.5	**Serviços Técnicos Especializados - ANALISTA DE SUPORTE Nível 2 (Hora Comercial - 08h de 2ª à 6ª das 06:00 às 22:00)**	**HORA HOMEM**	**104,10**	**60**		**6.246,00**		**24**		**149.904,00**
5.6	**Serviços de Manutenção, Suporte Técnico e Garantia**	**UNIDADE**	**212.507,44**	**1**		**212.507,44**		**24**		**5.100.178,56**
	TOTAL					**374.021,13**	**104.938.501,29**			**113.915.008,41**

ANEXO IV – PRÁTICAS PROIBIDAS

Práticas Proibidas

1.1 O Banco exige que todos os Mutuários (incluindo beneficiários de doações), Agências Executoras e Agências Contratantes, bem como, todas as empresas, entidades ou indivíduos que estejam atuando como proponentes ou participando de atividades financiadas pelo Banco incluindo, entre outros, requerentes, licitantes, proponentes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços, fornecedores de bens e concessionários (incluindo seus respectivos dirigentes, funcionários e agentes, independentemente de a agência ser expressa ou implícita), aderem os mais altos padrões éticos e denunciem ao Banco[1] qualquer ato suspeito de Práticas Proibidas sobre as quais tenham conhecimento ou venham tomar conhecimento tanto durante o processo de licitação e durante a negociação ou na execução de um contrato. As Práticas Proibidas compreendem: (i) práticas corruptas; (ii) práticas fraudulentas; (iii) práticas coercitivas; (iv) práticas colusivas; (v) práticas obstrutivas e (vi) apropriação indébita. O Banco estabeleceu mecanismos para denunciar suspeitas de Práticas Proibidas. Qualquer denúncia deverá ser encaminhada ao Escritório de Integridade Institucional (EII) do Banco para que se realize a devida investigação. O Banco também tem adotado procedimentos de sanções para julgar casos. Além disso, o Banco firmou com outras Instituições Financeiras Internacionais (IFIs) um acordo de reconhecimento mútuo de decisões de exclusão.

(a) O Banco define, para os fins desta disposição, os seguintes termos:
(i) uma prática corrupta consiste em oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer coisa de valor para influenciar indevidamente as ações de outra parte;
(ii) uma prática fraudulenta é qualquer ato ou omissão, incluindo a tergiversação de fatos ou circunstâncias que deliberada ou imprudentemente engane ou tente enganar, uma parte para obter um benefício financeiro ou de outra natureza ou para evitar cumprir uma obrigação;
(iii) uma prática coercitiva consiste em prejudicar ou causar dano, ou ameaçar prejudicar ou causar dano, direta ou indiretamente, a qualquer parte interessada ou à sua propriedade, para influenciar indevidamente as ações de uma parte;
(iv) uma prática colusiva é um acordo entre duas ou mais partes com o intuito de alcançar um propósito impróprio, inclusive influenciar inapropriadamente as ações de outra parte;
(v) Uma prática obstrutiva é:
i. destruir, falsificar, alterar ou ocultar evidências significativas de uma investigação do Grupo BID ou prestar declarações falsas aos investigadores com a intenção de obstruir uma investigação do Grupo BID;
ii. ameaçar, assediar ou intimidar qualquer parte interessada para impedi-la de revelar seu conhecimento sobre assuntos relevantes para uma investigação do Grupo BID ou ao seu prosseguimento; ou
iii. atos que visem impedir o exercício dos direitos contratuais de auditoria ou inspeção do Grupo BID previstos nas IAL 1.1 (f) abaixo ou seus direitos de acesso à informação; e
(vi) uma apropriação indébita consiste no uso de fundos ou recursos do Grupo BID para um propósito impróprio ou não autorizado, cometido intencionalmente ou por negligência grave.
(b) Se o Banco determinar que em qualquer estágio da aquisição ou da execução de um contrato qualquer empresa, entidade ou indivíduo que concorra ou participe de uma atividade financiada pelo Banco, incluindo, entre outros, requerentes, licitantes, proponentes, fornecedores de bens, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços, concessionários, Mutuários (incluindo Beneficiários de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos dirigentes, funcionários e agentes, independentemente de a agência ser expressa ou implícita) envolvidos em uma Prática Proibida, o Banco poderá:
(i) não financiar nenhuma recomendação de adjudicação de um contrato para obras, bens e serviços correlatos financiados pelo Banco;
(ii) suspender os desembolsos da operação se for determinado, em qualquer etapa, que um funcionário, agente ou representante do Mutuário, da Agência Executora ou Agência Contratante se envolveu em Prática Proibida;
(iii) declarar a Aquisição Viciada (Misprocurement) e cancelar e/ou declarar vencido antecipadamente o pagamento da parte do empréstimo ou da doação destinada a um contrato, quando houver evidências de que o representante do Mutuário ou do Beneficiário de uma doação não tomou as medidas corretivas adequadas (incluindo, entre outras, fornecer a notificação adequada ao Banco após tomar conhecimento da Prática Proibida) dentro de um prazo que o Banco considere razoável; (iv) emitir uma advertência à empresa, entidade ou indivíduo através de uma carta formal de censura por sua conduta;
(v) declarar que uma empresa, entidade ou indivíduo é inelegível, permanentemente ou por um prazo determinado, para: (i) receber ou participar em atividades financiadas pelo Banco; e (ii) ser designado[2] como subconsultor, subempreiteiro, fornecedor de bens ou prestador de serviços de uma empresa elegível à qual tenha sido adjudicado um contrato financiado pelo Banco;
(vi) encaminhar o assunto às autoridades competentes, encarregadas de fazer cumprir as leis; e/ou
(vii) impor outras sanções que julgar apropriadas sob as circunstâncias, incluindo a imposição de multas que representem o reembolso do Banco pelos custos associados às investigações e procedimentos. Essas sanções podem ser impostas adicionalmente ou em substituição às sanções mencionadas acima.
(c) As disposições dos incisos (i) e (ii) das IAL 1.1 (b) serão aplicadas, também, quando tais partes tiverem sido temporariamente declaradas inelegíveis para a adjudicação de novos contratos, enquanto aguardam a decisão definitiva de um processo de sanção ou de qualquer outra resolução.
(d) A imposição de qualquer ação a ser tomada pelo Banco de acordo com as disposições acima mencionadas, será pública.
(e) Além disso, qualquer empresa, entidade ou indivíduo que concorra ou participe de uma atividade financiada pelo Banco incluindo, entre outros, requerentes, licitantes, proponentes, fornecedores de bens, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços, concessionários, Mutuários (incluindo Beneficiários de doações), Agências Executoras ou Agências Contratante (incluindo seus respectivos dirigentes, funcionários e agentes, independentemente de a agência ser expressa ou implícita), podem estar sujeitos a sanções baseadas nos acordos que o Banco possa ter com outras IFIs em relação ao reconhecimento mútuo de decisões de exclusão. Para fins deste parágrafo, o termo "sanção" incluirá qualquer exclusão, condições sobre futuras contratações ou qualquer ação divulgada publicamente em resposta a uma violação da estrutura aplicável de uma IFI para tratar de alegações de Práticas Proibidas.
(f) O Banco exige que seja incluída uma disposição nos documentos de licitação e nos contratos financiados com um empréstimo ou doação do Banco, exigindo que os requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços e concessionários, permitam que o Banco inspecione todas e quaisquer contas, registros e outros documentos relativos à apresentação de ofertas e execução de contrato bem como que sejam auditados por auditores nomeados pelo Banco. No âmbito desta política, os requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços e concessionários devem prestar plena assistência ao Banco em sua investigação. O Banco terá também o direito de requerer que, nos contratos por ele financiados com um empréstimo ou doação incluam uma disposição que obrigue os requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços e concessionários a: (i) mantenham todos os documentos e registros referentes às atividades financiadas pelo Banco por sete (7) anos após a conclusão do trabalho contemplado no respectivo contrato; e (ii) forneçam quaisquer documentos necessários à investigação de alegações de Práticas Proibidas; e assegurem que funcionários ou agentes dos requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, subempreiteiros, subconsultores, prestadores de serviços ou concessionários que tenham conhecimento das atividades financiadas pelo Banco estejam disponíveis para responder às questões dos funcionários do Banco ou de qualquer investigador, agente, auditor ou consultor relacionado com a investigação devidamente designado. Caso o requerente, licitante, proponente, fornecedor de bens e seus agentes, empreiteiro, consultor, funcionários, subempreiteiro, subconsultor, prestador de serviços ou concessionário se recusem a cooperar e/ou descumpram o exigido pelo Banco ou obstruam de qualquer forma, a investigação, o Banco, a seu critério exclusivo, pode tomar as medidas apropriadas contra o requerente, licitante, proponente, fornecedor de bens e seus agentes, empreiteiro, consultor, funcionários, subempreiteiro, subconsultor, prestador de serviços ou concessionário.
(g) O Banco exigirá que, quando um Mutuário selecionar uma agência especializada para fornecer serviços de assistência técnica, todas as disposições relacionadas às Práticas Proibidas e as sanções correspondentes, serão aplicadas integralmente aos requerentes, licitantes, proponentes, empreiteiros, empresas de consultoria e consultores individuais, funcionários, subempreiteiros, subconsultores, prestadores de serviços ou fornecedores de bens, (incluindo seus respectivos dirigentes, funcionários e agentes,

independentemente de a agência ser expressa ou implícita), ou qualquer outra entidade que tenha assinado contratos com essa agência especializada para fornecer bens ou prestar serviços correlatos relacionados com as atividades financiadas pelo Banco. O Banco mantém o direito de exigir que o Mutuário invoque recursos tais como suspensão ou extinção. As agências especializadas deverão consultar a lista do Banco de empresas e indivíduos suspensos ou excluídos. No caso de uma agência especializada assinar um contrato ou uma ordem de compra com uma empresa ou com um indivíduo suspenso ou excluído pelo Banco, o Banco não financiará as despesas relacionadas e aplicará outras medidas conforme apropriado.
1.2 Com a concordância específica do Banco, além da Lista do Banco de Empresas e Indivíduos Sancionados, o Mutuário pode introduzir, nos formulários da Oferta e para contratos financiados pelo Banco, um compromisso do Licitante de observar, ao concorrer e executar um contrato, as leis e o sistema de sanções do país contra Práticas Proibidas (incluindo suborno) e os regulamentos e sanções de um organismo de desenvolvimento multilateral/bilateral ou organização internacional, atuando como cofinanciador, relacionados a práticas proibidas, se aplicável, conforme listado nos documentos de licitação³. O Banco aceitará a introdução de tal compromisso a pedido do país Mutuário, desde que as disposições que regem tal requisito sejam satisfatórias para o Banco).

PAÍSES ELEGÍVEIS

Elegibilidade para o Fornecimento de Bens, Construção de Obras
e Prestação de Serviços nas aquisições financiados pelo Banco

Nota: As referências ao Banco nesses documentos incluem o BID, o Laboratório do BID e qualquer fundo administrado pelo Banco.

A seguir, são apresentadas 2 opções do item número “1”, para que o Usuário escolha a que mais lhe convém, de acordo com a fonte de financiamento. Essa fonte pode ser o Banco Interamericano de Desenvolvimento (BID), o Laboratório de Licitações ou, ocasionalmente, os contratos podem ser financiados por fundos especiais que podem incluir diferentes critérios de elegibilidade para um determinado grupo de países-membros. Quando a última opção é selecionada, os critérios de elegibilidade devem ser mencionados nela:

---
1) Países-membros quando a fonte de financiamento é o Banco Interamericano de Desenvolvimento:
Alemanha, Argentina, Áustria, Bahamas, Barbados, Bélgica, Belize, Bolívia, Brasil, Canadá, Chile, Colômbia, Costa Rica, Croácia, Dinamarca, Equador, El Salvador, Eslovênia, Espanha, Estados Unidos, Finlândia, França, Guatemala, Guiana, Haiti, Honduras, Israel, Itália, Jamaica, Japão, México, Nicarágua, Noruega, Países Baixos, Panamá, Paraguai, Peru, Portugal, Reino Unido, República da Coreia, República Dominicana, República Popular da China, Suécia, Suíça, Suriname, Trinidade e Tobago, Uruguai, e Venezuela.
Territórios elegíveis
(a) Guadalupe, Guiana Francesa, Martinica, Reunião – por ser Departamentos da França.
(b) Ilhas Virgens dos EUA, Porto Rico, Guam - como Território dos Estados Unidos da América
(c) Aruba - como país constituinte do Reino dos Países Baixos; e Bonaire, Curaçao, Sint Maarten, Sint Eustatius - por serem Departamentos do Reino dos Países Baixos.
(d) Hong Kong - por ser uma Região Administrativa Especial da República Popular da China.

---

1) Lista de países quando um Fundo administrado pelo Banco está financiando:

(Incluir a lista de países)]

---

2) Critérios para determinar a nacionalidade e o país de origem dos bens e serviços

Para determinar: (a) a nacionalidade das empresas e indivíduos elegíveis para participar de contratos financiados pelo Banco e (b) o país de origem dos bens e serviços, serão usados os seguintes critérios:

(A) Nacionalidade

(a) Um indivíduo é considerado nacional de um país-membro do Banco se satisfaz um dos seguintes requisitos:
(i) é cidadão de um país-membro; ou
(ii) estabeleceu seu domicílio em um país-membro como residente de “boa-fé” e está legalmente autorizado para trabalhar nesse país.

(b) Uma empresa tem a nacionalidade de um país-membro se satisfizer os dois requisitos a seguir:
(i) está legalmente constituída ou estabelecida conforme as leis de um país-membro do Banco; e
(ii) mais de cinquenta por cento (50%) do capital da empresa é de propriedade de indivíduos ou empresas de países-membros do Banco.

Todos os sócios de uma associação em participação, associação, consórcio ou sociedade (ACS) com responsabilidade conjunta e solidária e todos os subempreiteiros devem cumprir os requisitos estabelecidos acima.

(B) Origem dos Bens

Os bens têm origem em um país-membro do Banco se foram extraídos, cultivados, colhidos ou produzidos em um país-membro do Banco. Considera-se que um bem é produzido quando, mediante manufatura, processamento ou montagem, o resultado é um

artigo comercialmente reconhecido cujas características, funções ou finalidades de uso são substancialmente diferentes de suas partes ou componentes.

No caso de um bem que consiste em vários componentes individuais que devem ser interconectados (pelo fornecedor, comprador ou um terceiro) para que o bem possa ser utilizado, e sem importar a complexidade da interconexão, o Banco considera que este bem é elegível para o financiamento se a montagem dos componentes tiver sido feita em um país-membro. Quando o bem é uma combinação de vários bens individuais que normalmente são empacotados e vendidos comercialmente como uma só unidade, o bem é considerado proveniente do país onde este foi empacotado e embarcado com destino ao comprador.

Para fins de determinação da origem dos bens identificados como “feito na União Europeia”, estes serão elegíveis sem necessidade de identificar o correspondente país específico da União Europeia.

A origem dos materiais, partes ou componentes dos bens ou a nacionalidade da empresa produtora, montadora, distribuidora ou vendedora dos bens não determina a origem dos mesmos.

(C) Origem dos Serviços

O país de origem dos serviços é o mesmo do indivíduo ou empresa que presta os serviços, conforme os critérios de nacionalidade acima estabelecidos. Este critério é aplicado aos serviços conexos ao fornecimento de bens (tais como transporte, seguro, instalação, montagem, etc.), aos serviços de construção e aos serviços de consultoria.

[1] No website do Banco (www.iadb.org/integridad), são encontradas informações sobre como denunciar supostas alegações de Práticas Proibidas, as normas aplicáveis ao processo de investigação e sanção, e o acordo que rege o reconhecimento mútuo de decisões de exclusão entre as Instituições Financeiras Internacionais.

[2] Um subconsultor, subempreiteiro, fornecedor de bens ou prestador de serviços nomeado (nomes diferentes podem ser utilizados dependendo do documento de licitação específico) é aquele que: (i) foi indicado pelo licitante em sua pré-qualificação ou oferta porque traz experiência e know-how específicos e cruciais que permitem ao licitante atender às exigências de qualificação para a licitação em questão; ou (ii) foi indicado pelo Mutuário.

[3] Por exemplo, tal compromisso pode ser redigido da seguinte forma: “Comprometemo-nos, no decorrer do processo licitatório (e durante a execução do contrato, caso nos seja adjudicado), a observar estritamente a legislação contra Práticas Proibidas (inclusive suborno) em vigor no país de [Agência Contratante], e os regulamentos e sanções de um organismo de desenvolvimento multilateral/bilateral ou organização internacional, atuando como cofinanciador, conforme essas leis e normas tenham sido incluídas por [Agência Contratante] nos documentos de licitação para este contrato e, sem prejuízo dos procedimentos do Banco para lidar com casos de Práticas Proibidas, aderir às normas administrativas estabelecidas por [autoridade local] para receber e resolver todas as reclamações relativas aos procedimentos de licitação.”

Documento assinado eletronicamente por **Shaaly Rodrigues Leite de Souza Lima**, **Assessor**, em 06/12/2024, às 17:06, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thiago Waltz**, **Diretor**, em 06/12/2024, às 17:18, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Gileno Gurjao Barreto**, **Diretor Presidente**, em 06/12/2024, às 17:22, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Paula Vitória Pereira**, **Coordenadora**, em 06/12/2024, às 17:33, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Julio Signorini**, **Assessor Técnico de Gabinete**, em 06/12/2024, às 17:33, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Daniel Medeiros Dantas Gomes**, **Coordenador**, em 06/12/2024, às 17:55, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thais Priscila de Sousa e Silva**, **Executiva Pública**, em 06/12/2024, às 18:02, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Marina Breviglieri Leite**, **Executiva Pública**, em 06/12/2024, às 18:06, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0048991888** e o código CRC **CB40052D**.