COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO

- P R O D E S P -

Taboão da Serra, 22 de Julho de 2026

PREGÃO ELETRÔNICO N° 90036/2026

COMUNICADO N° I

A PRODESP comunica a substituição da íntegra do “Anexo IX” – Minuta de Contrato do edital do Pregão Eletrônico n° 90036/2026, mantidas todas as demais condições do edital.

Em razão da modificação procedida fica designada a nova data de realização da sessão pública para o dia **07** / **08** / **2026** às **09** h **00**.

As demais datas do cronograma constam alteradas na página 02 do edital.

_____

Jorge Luiz de Souza
Matrícula n° 16053.3
Gerência de Licitações e Suporte Administrativo

PREGÃO ELETRÔNICO PRODESP N° 90036/2026
Edital n° 004/2026 (compras.gov.br)

Torna-se público que a **CIA. DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP**, conforme especificado neste Edital, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei federal 13.303/2016, pelo Regulamento Interno de Licitações e Contratos da PRODESP e demais normas da legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital e nos seus anexos.

PREGÃO ELETRÔNICO PRODESP N° 90036/2026

(UASG): 533201 - CIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP

Endereço: Rua Agueda Gonçalves, 240 – Jardim Pedro Gonçalves – Taboão da Serra – São Paulo – CEP. 06760-900

Processo n° 359.00000183/2026-11

OBJETO: Contratação de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação, controles de privacidade de dados, conforme as especificações e exigências descritas no Termo de Referência – **Anexo I**.

DATA E HORA DA ABERTURA DA SESSÃO PÚBLICA: 07 / 08 / 2026 – às 09h.

CRITÉRIO DE JULGAMENTO: Menor Preço Global

MODO DE DISPUTA: Aberto

LICITAÇÃO DE PARTICIPAÇÃO RESTRITA OU DE COTA RESERVADA ÀS ME/EPP/EQUIPARADAS: NÃO

CONSULTA AO EDITAL: O Edital e seus anexos estão disponíveis, na íntegra, no Portal de Compras do Governo Federal (www.gov.br/compras) e nos endereços eletrônicos www.prodesp.sp.gov.br – opção "fornecedores – editais de licitação e www.doe.sp.gov.br, opção "e-negociospublicos".

CRONOGRAMA

23/07/2026 - Publicação do Aviso de Licitação

03/08/2026 - Prazo Limite para envio de Esclarecimentos e Impugnações

06/08/2026 - Prazo Limite para resposta de Esclarecimentos e Impugnações

07/08/2026 - Abertura da Sessão Pública

1. OBJETO

1.1. Contratação de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação, controles de privacidade de dados, nível de conformidade com NIST CSF v2 & AI RMF (Artificial Intelligence Risk Management Framework), NIST SP 800-30 - Avaliação de Risco (Risk Assessments), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, *CIS Controls v8 Center for Internet Security, ISO 27001 -Information Security, Cybersecurity and Privacy protection , Cyber Insurance*, ISO 27701 *-Privacy Information Management*, ISO 27005 - *Information Security Risk Management*, ISSO 22301 - *Business continuity management systems*, ISO 23894 - *Artificial intelligence — Guidance on risk management*, apontamento por meio de inteligência artificial das melhores práticas de melhorias/sugestões com integração de ferramentas de segurança da informação e consultoria especializada em cibersegurança, conforme as especificações e exigências descritas no Termo de Referência – **Anexo I** do Edital.

1.1.1. O objeto da presente licitação enquadra-se como empreitada por preço unitário.

1.2. Em caso de discordância entre as especificações do código do item descrito no portal de compras do Governo Federal e as especificações constantes deste Edital, prevalecerão sempre as do Edital.

1.3. O valor estimado da presente contratação é sigiloso, nos termos do artigo 34, da Lei federal nº 13.303/2016, sendo a origem do recurso: Empresa não dependente – Fonte 4 recurso próprio e/ou Fonte 6 – Outras Fontes – Convênio Poupatempo e Convênio Acessa São Paulo.

2. CONDIÇÕES PARA PARTICIPAÇÃO

2.1. Poderão participar deste pregão os interessados que estejam regularmente credenciados no Sistema de Cadastramento Unificado de Fornecedores (SICAF) e no sistema eletrônico do Portal Nacional de Compras do Governo Federal (www.gov.br/compras).

2.2. As licitantes e seus representantes legais deverão estar previamente cadastrados no Portal de Compras do Governo Federal, antes da data de realização do Pregão, devendo credenciar-se no SICAF – Sistema de Cadastramento Unificado de Fornecedores, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil.

2.3. As informações sobre o cadastramento e credenciamento nos sistemas deverão ser obtidas no site www.gov.br/compras e nos Manuais disponíveis para consulta e impressão naquele site.

2.4. É de responsabilidade da licitante conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Não será admitida a participação, neste certame licitatório, de pessoas físicas ou jurídicas:

2.5.1. Que estejam com o direito de licitar e contratar temporariamente suspenso, ou que tenham sido impedidas de licitar e contratar com a Administração Pública estadual, direta e indireta;

2.5.2. Que tenham sido declaradas inidôneas pela Administração Pública federal, estadual ou municipal;

2.5.3. Que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativamente ou judicialmente;

2.5.4. Que estejam reunidas em consórcio ou sejam controladoras, coligadas ou subsidiárias entre si;

2.5.5. Que tenham sido proibidas pelo Plenário do CADE de participar de licitações promovidas pela Administração Pública federal, estadual, municipal, direta e indireta, em virtude de prática de infração à ordem econômica, nos termos do artigo 38, inciso II, da Lei federal n° 12.529/2011;

2.5.6. Que estejam proibidas de contratar com a Administração Pública em virtude de sanção restritiva de direito decorrente de infração administrativa ambiental, nos termos do art. 72, § 8°, inciso V, da Lei federal n° 9.605/1998;

2.5.7. Que estejam proibidas de contratar com o Poder Público em razão de condenação por ato de improbidade administrativa, nos termos do artigo 12 da Lei federal n° 8.429/1992, com redação dada pela Lei nº 14.230/2021;

2.5.8. Que tenham sido declaradas inidôneas para contratar com a Administração Pública pelo Plenário do Tribunal de Contas do Estado de São Paulo, nos termos do artigo 108 da Lei Complementar Estadual n° 709/1993;

2.5.9. Que tenham sido suspensas temporariamente, impedidas ou declaradas inidôneas para licitar ou contratar com a Administração Pública estadual, direta e indireta, por desobediência à Lei de Acesso à Informação, nos termos do artigo 33, incisos IV e V, da Lei federal n° 12.527/2011 e do artigo 62, incisos IV e V, do Decreto Estadual n° 68.155/2023;

2.5.10. Que estejam proibidas de participar da licitação ou de celebrar a contratação em decorrência do efeito de sanção registrada no Cadastro Nacional de Empresas Punidas – CNEP (artigo 22 da Lei federal n° 12.846/2013), ou no Cadastro Estadual de Empresas Punidas – CEEP (artigo 37 do Decreto estadual n° 67.301/2022);

2.5.11. Que sejam sociedades cooperativas, tendo em vista a vedação constante do § 1° do artigo 1° do Decreto Estadual n° 55.938, de 21 de junho de 2010, com a redação dada pelo Decreto Estadual n° 57.159, de 21 de julho de 2011;

2.5.12. Que incidam em quaisquer das vedações previstas no artigo 38, da Lei federal n° 13.303/2016.

2.6. Em relação à incidência das regras de tratamento favorecido a microempresas, empresas de pequeno porte e equiparadas, observa-se que:

2.6.1. A participação nesta licitação é ampla, sendo aplicáveis as regras de tratamento favorecido constantes dos artigos 42 a 45 da Lei Complementar federal n° 123/2006.

2.6.2. As microempresas e empresas de pequeno porte impedidas de optar pelo Simples Nacional, ante as vedações previstas na Lei Complementar n°

123/2006, não poderão aplicar os benefícios decorrentes desse regime diferenciado em sua proposta, devendo elaborá-la de acordo com as normas aplicáveis às demais pessoas jurídicas, sob pena de não aceitação dos preços ofertados pelo Pregoeiro.

2.6.2.1. Caso venha a ser contratada, a microempresa ou empresa de pequeno porte na situação descrita no item 2.6.2. deverá requerer ao órgão fazendário competente a sua exclusão do Simples Nacional até o último dia útil do mês subsequente àquele em que celebrada a contratação, nos termos do artigo 30, *caput,* inciso II, e §1°, inciso II, da Lei Complementar federal n° 123/2006, apresentando à Administração a comprovação da exclusão ou o seu respectivo protocolo.

2.6.2.2. Se a contratada não realizar espontaneamente o requerimento de que trata o item 2.6.2.1. caberá ao ente público contratante comunicar o fato ao órgão fazendário competente, solicitando que a empresa seja excluída de ofício do Simples Nacional, nos termos do artigo 29, inciso I da Lei Complementar federal n° 123/2006.

2.7. Cada representante credenciado poderá representar apenas uma licitante em cada pregão eletrônico.

2.8. O envio da proposta vinculará a licitante ao cumprimento de todas as condições e obrigações inerentes ao certame.

3. PROPOSTAS

3.1. As propostas deverão ser enviadas por meio eletrônico disponível no Portal de Compras do Governo Federal, endereço www.gov.br/compras, desde a divulgação da íntegra do Edital no referido endereço eletrônico até o dia e horário previstos no preâmbulo para a abertura da sessão pública, devendo a licitante, para formulá-las, assinalar a declaração de que cumpre integralmente os requisitos de habilitação constantes do Edital.

3.2. Os preços unitários e total serão ofertados no formulário eletrônico próprio, em moeda corrente nacional, em algarismos, apurado nos termos do item 3.3, sem inclusão de qualquer encargo financeiro ou previsão inflacionária. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas e custos diretos ou indiretos relacionados ao fornecimento do objeto, tais como tributos, remunerações, despesas financeiras e quaisquer outras necessárias ao cumprimento do objeto desta licitação, inclusive gastos com transporte.

3.2.1. As propostas não poderão impor condições e deverão limitar-se ao objeto desta licitação, sendo desconsideradas quaisquer alternativas de preço ou qualquer

outra condição não prevista no Edital e seus anexos.

3.2.2. A licitante deverá 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, tais como aumentos de custos de mão de obra decorrentes de negociação coletiva ou de dissídio coletivo de trabalho.

3.3. A proposta de preço deverá ser formulada com base nos valores vigentes na data-limite para a sua apresentação, a qual será considerada, para todos os efeitos, como data de referência de preços, nos termos do §1º do artigo 3º da Lei Federal nº 10.192/2001.

3.4. O prazo de validade da proposta será de 60 (sessenta) dias contados a partir da data de sua apresentação.

4. HABILITAÇÃO

4.1. Os documentos exigidos para fins de habilitação poderão, quando possível, ser substituídos por registro no Sistema de Registro Cadastral Unificado de Fornecedores (SICAF).

4.2. O julgamento da habilitação se processará mediante o exame dos documentos a seguir relacionados:

4.2.1. Habilitação jurídica

a) Registro empresarial na Junta Comercial, no caso de empresário individual;

b) Ato constitutivo, estatuto ou contrato social atualizado e registrado na Junta Comercial, em se tratando de sociedade empresária;

c) Documentos de eleição ou designação dos atuais administradores, tratando-se de sociedades empresárias;

d) Ato constitutivo atualizado e registrado no Registro Civil de Pessoas Jurídicas, tratando-se de sociedade não empresária, acompanhado de prova da diretoria em exercício;

e) Decreto de autorização, tratando-se de sociedade empresária estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

4.2.2. Regularidade fiscal e trabalhista

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, relativo à sede ou domicílio da licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

c) Certificado de regularidade do Fundo de Garantia por Tempo de Serviço (CRF - FGTS);

d) Certidão negativa, ou positiva com efeitos de negativa, de débitos trabalhistas (CNDT);

e) Certidão negativa, ou positiva com efeitos de negativa, de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União;

f) Certidão emitida pela Fazenda Municipal da sede ou domicílio da licitante que comprove a regularidade de débitos tributários relativos ao Imposto sobre Serviços de Qualquer Natureza – ISSQN.

4.2.3. Qualificação econômico-financeira

a) Certidão negativa de falência, recuperação judicial, expedida pelo distribuidor da sede da pessoa jurídica ou do domicílio do empresário individual;

a.1) Se a licitante for sociedade não empresária, a certidão mencionada na alínea "a" deverá ser substituída por certidão cujo conteúdo demonstre a ausência de insolvência civil, expedida pelo distribuidor competente.

a.2) Caso a licitante esteja em recuperação judicial, deverá ser comprovado o acolhimento do plano de recuperação judicial.

b) Demonstrações financeiras completas do último exercício social, exigíveis e apresentados na forma da Lei e normas contábeis vigentes, vedada a substituição por balancetes ou balanços provisórios.

b.1) No caso de empresa constituída há menos de ano, admite-se a apresentação de demonstrações financeiras completas referentes ao período de existência da sociedade;

b.2) As sociedades por ações deverão apresentar as demonstrações financeiras publicadas, de acordo com a legislação pertinente;

b.3) Entidades qualificadas como de grande porte, nos termos da Lei n° 11.648/2007, deverão evidenciar que as demonstrações financeiras apresentadas foram apreciadas por auditores independentes registrados na Comissão de Valores Mobiliários – CVM. A evidência poderá consistir em declaração emitida e assinada pelo auditor responsável pela análise das demonstrações financeiras ou, preferencialmente, no relatório do auditor independente, o qual poderá estar anexado às respectivas demonstrações financeiras.

b.4) Na hipótese de enquadramento no item b.3), a PRODESP poderá consultar o cadastro do auditor independente junto à CVM, o qual deverá estar devidamente ativo durante a execução dos trabalhos de auditoria das respectivas demonstrações financeiras, considerando-se como marco temporal final a data de conclusão dos trabalhos de auditoria ou a data de emissão do relatório do auditor independente, conforme aplicável.

b.5) Admite-se a apresentação de Balanço Patrimonial e Demonstrações do Resultado do Exercício extraídas da Escrituração Contábil Digital (ECD) em conjunto com os Termos de Abertura e Encerramento da Escrituração e recibo de transmissão. Nessa hipótese, à critério da PRODESP, poderão ser exigidas as demonstrações financeiras completas.

c) A capacidade econômica e financeira da licitante será atestada pelo atendimento a seguir:

c.1) A licitante deverá apresentar, por meio de declaração assinada por profissional habilitado da área contábil, os seguintes índices econômicos: i) LC = Liquidez Corrente; ii) LG = Liquidez Geral; e iii) SG – Solvência Geral, iguais ou superiores a 1 (um), sendo:

$$\text{Liquidez Geral} = \frac{\text{(Ativo Circulante + Realizável a Longo Prazo)}}{\text{(Passivo Circulante + Exigível a Longo Prazo)}}$$

$$\text{Liquidez Corrente} = \frac{\text{(Ativo Circulante)}}{\text{(Passivo Circulante)}}$$

$$\text{Solvência Geral} = \frac{\text{(Ativo Circulante + Realizável a Longo Prazo)}}{\text{(Passivo Circulante + Passivo não Circulante)}}$$

c.2) Na hipótese de a licitante não atingir qualquer dos três índices econômicos previstos acima, a licitante deverá comprovar patrimônio líquido ou capital

social mínimo de 10% (dez por cento) do valor da proposta ofertada pela licitante, tratando-se de contratação de serviços de caráter continuado, o percentual deverá ser calculado sobre o valor estimado correspondente ao período de 12 (doze) meses.

4.2.4. Declarações e outras comprovações

4.2.4.1. Declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **Anexo III**, atestando que:

a) se encontra em situação regular perante o Ministério do Trabalho e Emprego no que se refere a observância do disposto no inciso XXXIII do artigo 7.º da Constituição Federal, na forma do Decreto Estadual nº 42.911/1998;

b) não se enquadra em nenhuma das vedações de participação na licitação do item 2.5. deste Edital;

c) não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do artigo 1º e no inciso III do artigo 5º da Constituição Federal.

4.2.4.2. Declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **Anexo IV**, afirmando que sua proposta foi elaborada de maneira independente e que conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, em atendimento à Lei Federal nº 12.846/2013 e ao Decreto Estadual nº 67.301/2022.

4.2.4.3. Em se tratando de microempresa ou de empresa de pequeno porte, declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **Anexo V**, declarando seu enquadramento nos critérios previstos no artigo 3º da Lei Complementar Federal n° 123/2006, bem como sua não inclusão nas vedações previstas no mesmo diploma legal.

4.2.4.4. **Comprovação da condição de ME/EPP.** Sem prejuízo da declaração exigida no item 4.2.4.3 e admitida a indicação, pela licitante, de outros meios e documentos aceitos pelo ordenamento jurídico vigente, a condição de microempresa ou de empresa de pequeno porte será comprovada da seguinte forma:

4.2.4.4.1. Se sociedade empresária, pela apresentação de certidão expedida pela Junta Comercial competente;

4.2.4.4.2. Se sociedade simples, pela apresentação da "Certidão de Breve Relato de Registro de Enquadramento de

Microempresa ou Empresa de Pequeno Porte", expedida pelo Cartório de Registro de Pessoas Jurídicas;

4.2.4.5. Para o caso de empresas em recuperação judicial: Declaração subscrita por representante legal da licitante, elaborada em papel timbrado, conforme modelo **Anexo VI**, atestando que está ciente de que no momento da assinatura do Contrato deverá apresentar cópia do ato de nomeação do administrador judicial ou se o administrador for pessoa jurídica, o nome do profissional responsável pela condução do processo e, ainda, declaração, relatório ou documento equivalente do juízo ou do administrador, de que a licitante está cumprindo o plano de recuperação judicial.

4.2.4.6. Declaração subscrita por representante legal da licitante, em conformidade com o modelo **Anexo VII**, atestando a inexistência de fato impeditivo para licitar ou contratar com a Administração, estando absolutamente regular no ponto de vista jurídico, financeiro, fiscal e trabalhista, inclusive perante o INSS/FGTS e em virtude da Lei federal n° 9605/98 e Decreto estadual n° 66.819/2022.

4.2.4.7. **Declaração de ciência** subscrita por representante legal da licitante, comprometendo-se a apresentar, por ocasião da celebração do contrato, a comprovação de ser Revenda Autorizada do fabricante dos produtos ofertados, conforme modelo **Anexo VIII.**

4.2.4.7.1. A comprovação da condição de Revenda Autorizada do fabricante, pela licitante, deverá ser efetuada mediante a apresentação de documentos hábeis, tais como: contrato, atestado emitido em nome da licitante pelo respectivo fabricante, carta de certificação de parceria, emitidos em nome do licitante pelo fabricante, a ser apresentado à PRODESP antes da assinatura do contrato, ficando a CONTRATADA sujeita à aplicação de penalidades contratuais em caso de descumprimento.

4.2.4.7.1.1. O fabricante fica isento de apresentar a Comprovação de Revenda Autorizada, para sua participação nesta licitação.

4.2.4.7.1.2. Serão aceitos documentos eletrônicos, desde que permitida a comprovação de suas autenticidades através de consulta na internet.

4.2.5. Qualificação técnica

4.2.5.1. A licitante deverá apresentar atestado(s) de bom desempenho anterior

em contrato(s) da mesma natureza e porte, de complexidade tecnológica e operacional igual ou superior, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que especifique(m) em seu objeto necessariamente os tipos de serviços realizados, com indicações das quantidades, prazo contratual, datas de início e término e local da prestação de serviços, contemplando a execução dos serviços elencados abaixo relacionados diretamente ao objeto desta contratação, atestando, inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais, para os itens de maior relevância da contratação conforme descrito a seguir:

Tecnologia/Produto	Quantidade solicitada no tópico 7 do Termo de Referência – Estimativa da demanda	Quantidade mínima exigida para habilitação técnica
Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede)	10.000	1.000

4.2.5.1.1. Será aceito o somatório de atestados para fins de comprovação da experiência exigida no subitem anterior;

4.2.5.1.2. Entende-se por mesma natureza e porte, atestado(s) de fornecimentos e serviços similares ao objeto da licitação, que demonstre(m) que a licitante realizou fornecimentos de características compatíveis com as constantes do Termo de Referência.

4.2.5.1.3. O(s) atestado(s) deverá(ão) conter a identificação da pessoa jurídica emitente.

4.2.5.1.4. PRODESP poderá realizar diligência para averiguação da autenticidade dos atestados;

4.2.5.1.5. Documento em língua estrangeira deverá estar acompanhado da tradução para língua portuguesa por tradutor juramentado.

4.3. Disposições gerais sobre os documentos de habilitação

4.3.1. Na hipótese de não constar prazo de validade nas certidões apresentadas, a Administração aceitará como válidas as expedidas nos 180 (cento e oitenta) dias

imediatamente anteriores à data de apresentação das propostas.

4.3.2. O Pregoeiro, a seu critério, poderá diligenciar para esclarecer dúvidas ou confirmar o teor das declarações solicitadas no item 4.2.4 deste Edital e das comprovações de qualificação econômico-financeira e de qualificação técnica (caso exigidas nos itens 4.2.3 e 4.2.5), aplicando-se, em caso de falsidade, as sanções penais e administrativas pertinentes.

4.3.2.1. As declarações referidas no item 4.2.4. deverão ser assinadas com a utilização de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil.

4.3.3. Se a licitante for a matriz, os documentos exigidos no item 4.2.2 deverão estar em nome da matriz, e, se for filial, os documentos exigidos no item 4.2.2 deverão estar em nome da filial que, na condição de licitante, executará o objeto da contratação, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

4.3.4. A licitante que se considerar isenta ou imune de tributos relacionados ao objeto da licitação, cuja regularidade fiscal seja exigida no presente Edital, deverá comprovar tal condição mediante a apresentação de declaração emitida pela correspondente Fazenda do domicílio ou sede, ou outra equivalente, na forma da lei.

5. SESSÃO PÚBLICA E JULGAMENTO

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. As licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

5.3. Aberta a sessão pública, fica facultado ao pregoeiro desclassificar as propostas que não sejam compatíveis com as especificações definidas para o objeto ou que não cumpram os requisitos formais estabelecidos neste Edital.

5.3.1. A desclassificação da proposta será fundamentada e registrada no sistema, acompanhado em tempo real por todos os participantes.

5.4. Iniciada a etapa competitiva, as licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de **R$ 18.000,00 (dezoito mil reais)** e incidirá sobre o preço global.

5.6. A licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.7. O pregoeiro poderá, durante a disputa, como medida excepcional, excluir a proposta ou o lance que possa comprometer, restringir ou frustrar o caráter competitivo do processo licitatório, mediante comunicação eletrônica automática via sistema.

5.8. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do pregão, o sistema eletrônico poderá permanecer acessível às licitantes para a recepção dos lances.

5.8.1. O pregoeiro, quando possível, dará continuidade à sua atuação no certame, sem prejuízo dos atos realizados.

5.8.2. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa e terá reinício somente decorridas 24 (vinte e quatro) horas após a comunicação aos participantes, no endereço eletrônico utilizado para divulgação.

5.9. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública.

5.9.1. A prorrogação automática da etapa de envio de lances, de que trata o item 5.9., será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.9.2. Não havendo novos lances na forma estabelecida nos itens 5.9. e 5.9.1., a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.10. Encerrada a etapa de lances da sessão pública sem a prorrogação automática pelo sistema, o pregoeiro poderá admitir o reinício da etapa de lances, em prol da consecução do melhor preço.

5.10.1. Após o reinício previsto no item 5.10., as licitantes serão convocadas para apresentar lances intermediários.

5.11. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta

for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos artigos 44 e 45 da Lei Complementar federal nº 123/2006.

5.11.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.11.2. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.11.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no item anterior.

5.11.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos itens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.12. Encerrada a etapa de lances, o pregoeiro deverá negociar com o autor da oferta de menor valor mediante troca de mensagens abertas no sistema, com vistas à redução do preço.

5.12.1. A negociação poderá ser feita com as demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando a primeira colocada, mesmo após a negociação, for desclassificada em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.12.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelas demais licitantes.

5.12.3. O resultado da negociação será divulgado a todas as licitantes e anexado aos autos do processo licitatório.

5.13. As demais licitantes poderão reduzir seus preços ao valor da proposta da licitante mais bem classificada. A apresentação de novas propostas não prejudica o resultado da licitação em relação ao licitante mais bem classificado.

5.14. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 02 (duas) horas, envie a proposta detalhada e adequada ao último lance ofertado após a negociação realizada, conforme a Planilha de Proposta – **Anexo II**, deste edital, assim como acompanhada da Declaração de Produtos a Serem Fornecidos, conforme o modelo do **Anexo I-A**.

5.14.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pela licitante antes de findo o prazo, ou de ofício, a critério do pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio da Planilha de Proposta - **Anexo II** e da Declaração de Produtos a Serem Fornecidos **– Anexo I-A**, partes integrantes deste edital.

5.15. Após a negociação do preço, o pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se a licitante provisoriamente classificada em primeiro lugar atende às condições de participação no certame, conforme previsto no item 2.5 deste Edital, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - Ceis, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta);

c) Cadastro Nacional de Empresas Punidas - Cnep, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta);

d) Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade – CNCIAI, do Conselho Nacional de Justiça (http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

e) Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções (http://www.esancoes.sp.gov.br);

f) Cadastro Estadual de Empresas Punidas – CEEP (http://www.servicos.controladoriageral.sp.gov.br/PesquisaCEEP.aspx); e

g) Relação de apenados publicada pelo Tribunal de Contas do Estado de São Paulo (https://www.tce.sp.gov.br/apenados).

6.2. A consulta ao cadastro especificado na alínea “d” do item 6.1 será realizada em nome da pessoa jurídica licitante e também de seu sócio majoritário, por força do artigo 12 da Lei federal n° 8.429/1992.

6.3. Caso conste na Consulta de Situação da licitante a existência de Ocorrências Impeditivas Indiretas, o pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de

fornecimento similares, dentre outros.

6.3.2. A licitante será convocada para manifestação previamente a uma eventual desclassificação.

6.3.3. Constatada a existência de sanção, a licitante será reputada inabilitada, por falta de condição de participação.

6.4. A análise das propostas pelo pregoeiro se limitará ao atendimento das condições estabelecidas neste Edital e seus anexos e à legislação vigente.

6.4.1. Serão desclassificadas as propostas:

a) que contiverem vícios insanáveis;

b) cujo objeto não atenda as especificações, prazos e condições fixados neste Edital;

c) que apresentem preço baseado exclusivamente em proposta das demais licitantes;

d) apresentadas por licitante impedida de participar, nos termos do item 2.5 deste Edital;

e) que apresentem preços unitários ou total simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos ou salários de mercado;

f) formuladas por licitantes participantes de cartel, conluio ou qualquer acordo colusivo voltado a fraudar ou frustrar o caráter competitivo do certame licitatório.

6.5. A aceitabilidade dos preços será aferida com base nos valores de mercado vigentes na data de referência de preços, apurados mediante pesquisa realizada pela PRODESP que será juntada aos autos por ocasião do julgamento. A verificação da exequibilidade do preço ofertado poderá observar, no que couber, os seguintes critérios:

6.5.1. Compatibilidade dos preços ofertados com os valores dos insumos praticados no mercado, coerentes com a execução do objeto da licitação, acrescidos dos respectivos tributos, encargos sociais, trabalhistas e previdenciários, benefícios e despesas indiretas, bem como com as determinações do Termo de Referência **– Anexo I**.

6.5.2. Será considerado manifestamente inexequível o preço que não venha a ter demonstrada sua viabilidade para a perfeita execução do contrato, com a comprovação de que os custos dos insumos são coerentes com os de mercado e com as determinações do Termo de Referência - **Anexo I**.

6.5.3. Verificada a hipótese de preço inexequível, será concedido o direito de contraditório à licitante, para comprovar a regularidade de sua proposta, sob pena de desclassificação.

6.5.4. A PRODESP poderá solicitar à licitante a apresentação de justificativa detalhada da forma utilizada para cálculo dos custos, a fim de comprovar sua exequibilidade, ficando a aceitação condicionada à análise do Pregoeiro, sobre a qual decidirá motivadamente.

6.5.5. Uma vez aceita a justificativa do cálculo pela PRODESP, a licitante assume inteira responsabilidade pelos itens de composição do preço e seus valores, para todos os efeitos, não podendo alegar provisão deficitária ou omissão com vistas à repactuação ou reequilíbrio econômico-financeiro, caso seja contratada.

6.5.6. O Pregoeiro poderá a qualquer momento solicitar às licitantes a composição de preços unitários de serviços e/ou de materiais/equipamentos, bem como os demais esclarecimentos que julgar necessários.

6.6. A desclassificação se dará por decisão motivada do Pregoeiro, observado o disposto no artigo 42 do Regulamento Interno de Licitações e Contratos da PRODESP.

6.7. Verificadas as condições de participação e de utilização de tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

6.7.1. Se a proposta vencedora for desclassificada, o pregoeiro examinará a proposta subsequente, e, assim sucessivamente, na ordem de classificação.

6.7.2. Encerrada a fase de julgamento, caso se verifique a conformidade da proposta de que trata o item 6.6, o pregoeiro passará à verificação da documentação de habilitação da licitante.

7. HABILITAÇÃO

7.1. Os documentos que serão exigidos para fins de habilitação estão especificados nos itens 4.2.1., 4.2.2., 4.2.3., 4.2.4. e 4.2.5. deste Edital, consistindo na documentação necessária e suficiente para demonstrar a capacidade da licitante de realizar o objeto da licitação.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Os documentos exigidos para fins de habilitação que não estejam contemplados no SICAF ou que estejam vencidos, deverão ser enviados na forma eletrônica por meio do sítio www.gov.br/compras.

7.3. A habilitação será verificada por meio do SICAF, nos documentos por ele abrangidos.

7.4. A verificação no SICAF ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.5. Durante a entrega dos documentos para habilitação, a licitante poderá enviar documentos para suprir eventuais omissões ou sanear falhas relativas ao cumprimento dos requisitos e condições de habilitação estabelecidos neste Edital mediante a apresentação de documentos, preferencialmente no campo próprio do Sistema Compras.gov, ou por correio eletrônico a ser fornecido pelo Pregoeiro no chat do sistema, desde que os envie no curso da própria sessão pública e antes de ser proferida a decisão sobre a habilitação.

7.5.1. Concluída a etapa referida no item 7.5. não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência para:

7.5.1.1. complementação de informações acerca dos documentos já apresentados pelas licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.5.1.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

7.6. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.7. Na hipótese de a licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente Edital.

7.8. A comprovação da regularidade fiscal e trabalhista de microempresas ou empresas de pequeno porte será exigida apenas para efeito de celebração da contratação. Não obstante, a apresentação de todas as certidões e documentos exigidos para a comprovação da regularidade fiscal e trabalhista será obrigatória na fase de habilitação, ainda que apresentem alguma restrição ou impedimento.

7.8.1. A prerrogativa tratada no item 7.8. abrange apenas a regularidade fiscal e trabalhista da licitante enquadrada como microempresa ou empresa de pequeno porte, não abrangendo os demais requisitos de habilitação exigidos neste Edital, os quais deverão ser comprovados durante o certame licitatório e na forma prescrita neste Edital.

8. RECURSO, ADJUDICAÇÃO E HOMOLOGAÇÃO.

8.1. Divulgado o vencedor, o Pregoeiro informará às licitantes por meio de mensagem lançada no sistema que poderão interpor recurso, imediata e motivadamente, por meio eletrônico, utilizando exclusivamente o campo próprio disponibilizado no sistema.

8.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos;

8.2. Havendo interposição de recurso o Pregoeiro informará aos recorrentes que poderão apresentar memoriais contendo as razões recursais no prazo de 03 (três) dias úteis após o encerramento da sessão pública, sob pena de preclusão. As demais licitantes poderão apresentar contrarrazões ao(s) recurso(s) interposto(s) no prazo comum de 03 (três) dias úteis contados a partir do término do prazo para apresentação, pelo(s) recorrente(s), dos memoriais recursais, sendo-lhes assegurada vista aos autos do processo na PRODESP, mediante prévia solicitação pelo endereço eletrônico cplprodesp@sp.gov.br.

8.3. Os memoriais de recurso e as contrarrazões serão oferecidos por meio eletrônico no sítio (www.gov.br/compras), no campo próprio disponibilizado no sistema. A apresentação de documentos relativos às peças antes indicadas, se houver, será efetuada mediante protocolo na PRODESP ou envio para o e-mail pregaoeletronicoprodesp@sp.gov.br, dentro dos prazos estabelecidos no item 8.2.

8.4. A falta de interposição do recurso na forma prevista no item 8.1.1. importará na decadência do direito de recorrer.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão ou encaminhar o recurso para a autoridade superior proferir sua decisão.

8.6. O recurso terá efeito suspensivo e o seu acolhimento importará a invalidação dos atos insuscetíveis de aproveitamento.

8.7. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto da licitação à licitante vencedora e homologará o procedimento licitatório.

8.8. A adjudicação será feita considerando a totalidade do objeto.

9. PRAZOS, LOCAIS E CONDIÇÕES DE ENTREGA

9.1. O objeto desta licitação deverá ser entregue em conformidade com as especificações constantes do Termo de Referência, que constitui o **Anexo I** deste Edital, correndo por conta da contratada as despesas necessárias à sua execução, em especial as relativas a seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto do contrato.

10. CONDIÇÕES DE RECEBIMENTO DO OBJETO

10.1. As condições de recebimento do objeto são aquelas definidas pelo termo de contrato, cuja minuta constitui o **Anexo IX** deste Edital.

11. PAGAMENTOS

11.1. Os pagamentos serão efetuados em conformidade com o termo de contrato, cuja minuta constitui o **Anexo IX** deste Edital.

12. CONTRATAÇÃO

12.1. A contratação decorrente deste certame licitatório será formalizada mediante a assinatura de termo de contrato, cuja minuta integra este Edital como **Anexo IX**.

12.1.1. Se, por ocasião da celebração do contrato, algum dos documentos apresentados pela adjudicatária para fins de comprovação da regularidade fiscal ou trabalhista estiver com o prazo de validade expirado, a PRODESP verificará a situação por meio eletrônico hábil de informações e certificará a regularidade nos autos do processo, anexando ao expediente os documentos comprobatórios, salvo impossibilidade devidamente justificada.

12.1.2. Se não for possível atualizar os documentos referidos no item 12.1.1 por meio eletrônico hábil de informações, a adjudicatária será notificada para, no prazo de 02 (dois) dias úteis, comprovar a sua situação de regularidade mediante a apresentação das certidões respectivas com prazos de validade em plena vigência, sob pena de a contratação não se realizar.

12.1.3. Constitui condição para a celebração da contratação, bem como para a realização dos pagamentos dela decorrentes, a inexistência de registros em nome da adjudicatária no "Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL". Esta condição será considerada cumprida se a devedora comprovar que os respectivos registros se encontram suspensos, nos termos do artigo 8º, §§ 1º e 2º, da Lei Estadual nº 12.799/2008.

12.1.4. Com a finalidade de verificar o eventual descumprimento pela licitante das condições de participação previstas no item 2.5 deste Edital serão consultados, previamente à celebração da contratação, os cadastros referidos no item 6.1

12.1.5. Constituem, igualmente, condições para a celebração do contrato:

12.1.5.1. a apresentação do(s) documento(s) que a adjudicatária, à época do certame licitatório, houver se comprometido a exibir antes da celebração do contrato por meio de declaração específica, exigida no item 4.2.4.7. neste Edital.

12.2. A adjudicatária será convocada pela PRODESP para assinatura do termo de contrato no prazo de 5 (cinco) dias corridos, contados da data da convocação. O contrato será assinado com a utilização de meio eletrônico, nos termos da legislação aplicável. O

prazo para assinatura poderá ser prorrogado por igual período por solicitação justificada do interessado e aceita pela Administração.

12.3. As demais licitantes classificadas serão convocadas para participar de nova sessão pública do pregão, com vistas à celebração do contrato, quando a adjudicatária:

12.3.1. Deixar de comprovar sua regularidade fiscal e trabalhista, nos moldes do item 7.8, ou na hipótese de invalidação do ato de habilitação com base no disposto no item 7.5;

12.3.2. For convocada dentro do prazo de validade de sua proposta e não apresentar a situação regular de que tratam os itens 12.1.1 a 12.1.5 deste Edital.

12.3.3. Recusar-se a assinar o contrato ou não assinar o contrato no prazo e condições estabelecidos;

12.3.4. For impedida de participar desta licitação, nos termos do item 2.5. deste Edital;

12.4. A nova sessão de que trata o item 12.3 será realizada em prazo não inferior a 03 (três) dias úteis contados da publicação do aviso no Diário Oficial do Estado de São Paulo.

12.4.1. O aviso será também divulgado nos endereços eletrônicos www.prodesp.sp.gov.br e www.doe.sp.gov.br, opção “NEGÓCIOS PÚBLICOS”.

13. SANÇÕES ADMINISTRATIVAS

13.1. Estará sujeito às penalizações previstas no artigo 156, da lei federal n° 14.133/2021, quem convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, sendo assegurados o contraditório e a ampla defesa;

.

13.2. As sanções referidas no item 13.1. poderão ser aplicadas juntamente com as multas previstas no **Anexo IX** deste edital (Contrato), observados os princípios do devido processo legal, contraditório, ampla defesa, razoabilidade, proporcionalidade, segurança jurídica, interesse público, eficiência, bem como o dever de motivação das decisões proferidas, nos termos do artigo 85 do Regulamento Interno de Licitações e Contratos e deverão ser registradas no “Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções”, no endereço www.esancoes.sp.gov.br e também no “Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS”, no endereço http://www.portaltransparencia.gov.br/ceis;

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

13.4. O contratante poderá descontar das faturas os valores correspondentes às multas que eventualmente lhe forem aplicadas por descumprimento das obrigações estabelecidas neste Edital, seus anexos ou no termo de contrato, quando houver;

13.5. A prática de atos que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública, ou que de qualquer forma venham a constituir fraude ou corrupção, durante a licitação ou ao longo da execução do contrato, será objeto de instauração de processo administrativo de responsabilização nos termos da Lei Federal n° 12.846/2013 e do Decreto Estadual n° 67.301/2022, sem prejuízo da aplicação das sanções administrativas.

14. GARANTIA DE EXECUÇÃO CONTRATUAL

14.1. As condições de prestação de garantia de execução contratual são aquelas definidas pelo termo de contrato, cuja minuta constitui o **Anexo IX** deste Edital.

15. IMPUGNAÇÕES E PEDIDOS DE ESCLARECIMENTOS

15.1. Qualquer cidadão é parte legítima para pedir esclarecimentos ou impugnar o edital, no prazo de 03 (três) dias úteis anteriores à data designada para a abertura de certame. Os pedidos de esclarecimentos ou impugnação deverão ser realizados por forma eletrônica no endereço eletrônico cplprodesp@sp.gov.br, até as 23h59 da data limite estabelecida no CRONOGRAMA constante na página 2 deste edital.

15.2. O pregoeiro deverá apresentar os esclarecimentos e encaminhar à autoridade competente para responder a impugnação, motivadamente, até o dia útil anterior a data fixada para a abertura da sessão pública.

15.3. Serão desconsiderados os pedidos de esclarecimentos e impugnações apresentados além do prazo estabelecido no item 15.1.

15.4. As respostas aos pedidos de esclarecimento e impugnação, bem como demais informações relevantes, serão divulgadas mediante publicações no Portal de Compras do Governo Federal (www.gov.br/compras) e na página da PRODESP na Internet, no endereço www.prodesp.sp.gov.br.

16. DISPOSIÇÕES GERAIS

16.1. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitada a igualdade de oportunidade entre as licitantes, desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

16.2. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

16.2.1. As falhas passíveis de saneamento na documentação apresentada pela licitante são aquelas cujo conteúdo retrate situação fática ou jurídica já existente na data da abertura da sessão pública deste Pregão.

16.2.2. O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

16.2.3. À licitante caberá acompanhar as operações no sistema eletrônico durante a sessão pública, respondendo pelos ônus decorrentes de sua desconexão ou da inobservância de quaisquer mensagens emitidas pelo sistema.

16.3. Os prazos indicados neste Edital em dias corridos, quando vencidos em dia não útil, prorrogam-se para o dia útil subsequente.

17. ANEXOS

17.1. Integram o presente Edital:

Anexo I - Termo de Referência;

Anexo I-A - Declaração de Produtos a Serem Fornecidos;

Anexo II - Modelo de planilha de proposta;

Anexo III - Modelo de Declaração de Comprovação de Regularidade Perante o Ministério do Trabalho e Emprego;

Anexo IV - Modelo de Declaração – Marco Legal Anticorrupção;

Anexo V - Modelo de Declaração de Enquadramento como Microempresa ou Empresa de Pequeno Porte;

Anexo VI - Modelo de Declaração (empresas em recuperação judicial);

Anexo VII - Modelo de Declaração de Inexistência de Fato Impeditivo;

Anexo VIII - Modelo de Declaração de Ciência (Revenda Autorizada);

Anexo IX - Minuta de Contrato;

Anexo X - Regulamento Interno de Licitações e Contratos da Prodesp

Taboão da Serra, 20 de Julho de 2026

Jorge Luiz de Souza
Matrícula nº 16053.3
Gerência de Licitações e Suporte Administrativo

ANEXO I

TERMO DE REFERÊNCIA

ANEXO I-A

DECLARAÇÃO DE PRODUTOS A SEREM FORNECIDOS

Governo do Estado de São Paulo
Companhia de Processamento de Dados do Estado de São Paulo
Gerência de Negócios, Acordos e Contratos Estratégicos

TERMO DE REFERÊNCIA

Nº do Processo: 359.00000183/2026-41

Interessado: Gerência de Segurança da Informação

Assunto: Plataforma de segurança cibernética para avaliação de maturidade e nível de risco corpoprativo

ANEXO I

TERMO DE REFERÊNCIA

CONTRATAÇÃO DE PLATAFORMA DE GOVERNANÇA E MATURIDADE CIBERNÉTICA - SAAS

REL.GEX.011/2026 v.1.5 - Junho/2026

PREÂMBULO

CONTEÚDO DO ANEXOS

ANEXO I - TERMO DE REFERÊNCIA: fornece as especificações técnicas mínimas necessárias as quais o produto e/ou serviço ofertado pela proponente deverá obrigatoriamente atender.

ANEXO I-A - DECLARAÇÃO DE PRODUTOS A SEREM FORNECIDOS: deve ser entregue assinado pelo representante legal, conforme disposto no Contrato Social ou Estatuto, com carimbo ou identificação da assinatura, utilizando preferencialmente este Anexo. Qualquer observação de âmbito técnico deverá ser feita apenas no Anexo I-A.

ANEXO I-B - TERMO DE CONFIDENCIALIDADE, SIGILO E USO: fornece modelo do termo de confidencialidade, no qual a Contratada deverá apresentar após assinatura do contrato.

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação, controles de privacidade de dados, nível de conformidade com NIST CSF v2 & AI RMF (*Artificial Intelligence Risk Management Framework*), NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, *CIS Controls v8 Center for Internet Security, ISO 27001* -

Information Security, Cybersecurity and Privacy protection, *Cyber Insurance*, ISO 27701 - *Privacy Information Management*, ISO 27005 - *Information Security Risk Management*, ISO 22301 - *Business continuity management systems*, ISO 23894 - *Artificial intelligence — Guidance on risk management*, apontamento por meio de inteligência artificial das melhores práticas de melhorias/sugestões com integração de ferramentas de segurança da informação e consultoria especializada em cibersegurança.

2. VIGÊNCIA DO CONTRATO

2.1. A vigência do contrato será de **12 (doze) meses**, contados a partir da data de sua assinatura. A vigência contratual poderá ser prorrogada, caso haja interesse da PRODESP, até o limite estabelecido pelo art. 71 da Lei n.º 13.303/2016, exceto para os itens de serviços de Setup/Implantação e Transferência de Conhecimento (*Hands-On*).

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. A presente contratação tem como finalidade a disponibilização de uma plataforma integrada de gestão de riscos e conformidade em segurança da informação, alinhada às legislações e normas nacionais e internacionais de referência, a fim de apoiar a instituição na implementação, monitoramento e aprimoramento contínuo de sua governança cibernética.

3.2. A **Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD)** estabelece a obrigatoriedade de adoção de medidas técnicas e administrativas aptas a proteger dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Nesse contexto, a instituição deve comprovar sua aderência aos princípios da segurança da informação, privacidade e proteção de dados.

3.3. Paralelamente, normas e *frameworks* internacionais como a NIST CSF v2 & AI RMF (*Artificial Intelligence Risk Management Framework*), NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS *Controls* v8 *Center for Internet Security*, ISO 27001 - *Information Security*, *Cybersecurity and Privacy protection*, *Cyber Insurance*, ISO 27701 - *Privacy Information Management*, ISO 27005 - *Information Security Risk Management*, ISO 22301 - *Business continuity management systems*, ISO 23894 - *Artificial intelligence — Guidance on risk management*, estabelecem diretrizes e controles técnicos e administrativos reconhecidos mundialmente como boas práticas de cibersegurança.

3.4. A complexidade crescente do cenário tecnológico, somada ao aumento exponencial de incidentes cibernéticos (como vazamento de dados, ataques de ransomware, phishing e comprometimento de credenciais), demanda da Administração Pública mecanismos automatizados, inteligentes e integrados para:

- Avaliar riscos tecnológicos e corporativos de forma contínua e objetiva;
- Monitorar o grau de maturidade da segurança cibernética;
- Auditar processos, controles e conformidade;
- Integrar diferentes ferramentas de segurança (SIEM, SOC, DLP, IAM, firewalls, EDR/antivírus corporativos);
- Gerar relatórios gerenciais e técnicos que subsidiem decisões estratégicas e auditorias externas;

- Prover recomendações de melhorias com apoio de inteligência artificial (IA), possibilitando ajustes proativos, ágeis e baseados em melhores práticas reconhecidas.
- Geração de planos de ação baseados nos níveis de risco, conformidade, maturidade e melhorias.
- Lista de Indicadores Chave de Desempenho (KPI – *Key Performance Indicator*).
- Lista de Indicadores Chave de Objetivos (KGI – *Key Goal Indicator*).
- Geração de indicadores, planos de ação com a indicação de complexidade, ações, prioridade, projetos e grau de importância.

3.5. A justificativa da contratação encontra-se pormenorizada no Relatório de Justificativa (id. SEI n°0093760282) constante do processo SEI n.º 359.00000183/2026-41.

3.6. Alinhamento aos Instrumentos de Planejamento Institucionais

3.6.1. Alinhamento aos Planos Estratégicos:

OBJETIVO ESTRATÉGICO	REFERÊNCIA
VI - digitalizar o acesso a prestação de serviços públicos VIII - automatizar processos de trabalho, com foco na eficiência	Estratégia de Governo Digital - 2023-2026 (Art. 4º - Decreto n.° 67.799 de 13 de julho de 2023)
OE 1 - Fortalecer a marca PRODESP OE 3 - . Entregar com excelência, garantindo segurança, privacidade, disponibilidade e performance	Planejamento Estratégico -2024-2028

3.7. Alinhamento ao Plano Diretor de Tecnologia da Informação da Prodesp:

INICIATIVAS	REFERÊNCIA
21 - Oferecer produtos e soluções para transformação digital	Plano Diretor de Tecnologia da Informação da Prodesp - 2023-2026

3.8. Resultados e Benefícios a serem alcançados na oferta de produtos e servicos

3.8.1. Redução de Riscos Associados a Ataques Cibernéticos: A solução ajuda a identificar e corrigir vulnerabilidades, reduzindo significativamente os riscos de ataques cibernéticos e garantindo a proteção dos dados e sistemas da organização;

3.8.2. Conformidade com Regulamentações e Padrões de Segurança: A contratação de uma solução de segurança cibernética ajuda a garantir a conformidade com regulamentações e padrões de segurança, como ISO 27001, proporcionando maior segurança e confiança para a organização;

3.8.3. Gestão de riscos e conformidade;

3.8.4. Maior Eficiência Operacional das Equipes de Segurança: A solução proporciona ferramentas avançadas e automação por meio de integração com ferramentas de vulnerabilidades e orquestração em segurança da informação, aumentando a eficiência operacional das equipes de segurança e permitindo uma resposta mais rápida e eficaz a incidentes de segurança;

3.8.5. A possibilidade de benchmarking interno e externo, inclusive com padrões governamentais e setoriais;

3.8.6. Relatórios Detalhados e Contínuos: A solução oferece relatórios contínuos e detalhados para análise e melhoria da segurança, permitindo a identificação de vulnerabilidades e a implementação de medidas corretivas de forma proativa;

3.8.7. Suporte Técnico e Manutenção: A contratação inclui suporte técnico contínuo e manutenção ao longo dos 12meses, garantindo a operação eficiente e segura da solução de segurança cibernética.

4. DESCRIÇÃO DA SOLUÇÃO DE TIC

4.1. Para todos os efeitos do presente instrumento define-se como objeto a eventual contratação da Plataforma de Governança e Maturidade em Cibersegurança , para avaliação do nível de Risco Corporativo e Tecnológico, nível e monitoramento de Maturidade e Auditoria, governança de Segurança da Informação, privacidade de dados, tecnologias, nível de conformidade com NIST CSF v2 & AI RMF (*Artificial Intelligence Risk Management Framework*), NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS *Controls* v8 *Center for Internet Security*, ISO 27001 - *Information Security*, *Cybersecurity and Privacy protection*, *Cyber Insurance*, ISO 27701 - *Privacy Information Management*, ISO 27005 - *Information Security Risk Management*, ISO 22301 - *Business continuity management systems*, ISO 23894 - *Artificial intelligence — Guidance on risk management*, apontamento por meio de inteligência artificial das melhores práticas de melhorias/sugestões com integração de ferramentas de segurança da informação e consultoria especializada em cibersegurança.

4.2. **Assegurar conformidade legal e regulatória**

- Atender aos requisitos da LGPD baseados na ISO 27701, garantindo a adoção de medidas técnicas e administrativas necessárias à proteção de dados pessoais.
- Alinhar controles e processos aos referenciais normativos da a NIST CSF v2 NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias , & AI RMF (*Artificial Intelligence Risk Management Framework*), CIS *Controls* v8] *Center for Internet Security*, ISO 27001 - *Information Security*, *Cybersecurity and Privacy protection*, *Cyber Insurance*, ISO 27701 - *Privacy Information Management*, ISO 22301 - *Business continuity management systems*, ISO 23894 - *Artificial intelligence — Guidance on risk management*, elevando o padrão de segurança organizacional.

4.2.1. <u>Implantar uma Plataforma de Governança e Maturidade em Cibersegurança</u>

- Disponibilizar ambiente unificado para identificação, avaliação, classificação e priorização de riscos tecnológicos e corporativos.
- Oferecer dashboards executivos e relatórios detalhados para subsidiar decisões estratégicas e operacionais.
- Mapa de controles por tipo domínio (Governança, Identificação, Proteção, Detecção, Resposta e Recuperação).
- Uso para escolha do melhor framework e quais controles por Indicador global ou de desempenho.

4.2.2. Monitorar a maturidade em segurança cibernética

- Estabelecer indicadores e métricas que permitam mensurar a evolução do nível de maturidade organizacional em segurança da informação.
- Acompanhar planos de ação e evidenciar resultados em auditorias internas e externas.
- Definição de indicadores de risco
- Nível de exposição a vulnerabilidades críticas, severa e moderadas, com ponderação por criticidade e relação de risco com o CVSS (*Common Vulnerability Scoring System*)
- NIST CSF v2: Níveis *Partial* (1) a *Adaptive* (5).
- CMMI aplicado à segurança: níveis de 1 (Inicial) a 5 (Otimizado).
- CIS *Controls Implementation Groups* (IG1-IG3): progressão da adoção de controles básicos até avançados.

4.2.3. Automatizar auditorias e relatórios de conformidade

- Reduzir custos e tempo despendidos em auditorias tradicionais.
- Disponibilizar evidências documentais, registros e trilhas de auditoria que comprovem conformidade regulatória e melhores práticas adotadas.

4.2.4. Fortalecer a governança de privacidade e proteção de dados

- Garantir mecanismos para atendimento a direitos dos titulares de dados, como acesso, retificação e exclusão.
- Apoiar os profissionais de tecnologia da informação, executivos de TI e Segurança da informação, encarregados de dados e demais áreas responsáveis na execução de suas atribuições.

4.2.5. Acompanhamento do Plano de Ação

- Avaliação de Controles versus Requisitos.
- Identificação de lacunas e controles não realizados identificado.
- Geração de lista de pendências (*back-log*).
- Utilização de Ações corretivas em âmbito estratégico, tático e operacional.
- Relatórios de maturidade periódicos: mostrar evolução de métricas em períodos (trimestral, semestral).
- Evidências objetivas: logs de SIEM, relatórios de vulnerabilidade, atas de comitês de risco, certificados de treinamentos.
- Conformidade cruzada: mapear métricas e resultados contra frameworks (ex.: NIST GV.RM-01, ISO 27001 cláusula 9.1).
- Preparação para auditorias externas: manter documentação organizada, incluindo histórico de melhorias e planos de ação concluídos.

4.2.6. Aplicar inteligência artificial à cibersegurança.

- Disponibilizar recursos de análise preditiva para identificação de vulnerabilidades e tendências de ataques.
- Fornecer recomendações automáticas de melhorias e priorização de ações

corretivas e preventivas.

- Aplicar as medidas de controle baseados no NIST AI 100-1 e ISO ISO.23894-AI.

4.2.7. Integrar-se às soluções tecnológicas existentes

- Capacidade de integração técnica, sob demanda ou conforme a conveniência da contratante, via conectores nativos ou APIs, com as soluções corporativas preexistentes, tais como: SIEM, DLP, PAM/IAM, Antivírus, Gestão de Vulnerabilidades (SAST/DAST), Testes de Intrusão e EDR/XDR.
- Ampliar a eficiência operacional e reduzir redundâncias de investimento em múltiplas soluções isoladas.

4.2.8. Fortalecer a confiança institucional

- Demonstrar compromisso da instituição com segurança da informação, privacidade e conformidade.
- Ampliar a credibilidade junto a cidadãos, parceiros, fornecedores, órgãos de controle e sociedade em geral.

5. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

5.1. Da Especificação e Quantidade - LOTE ÚNICO

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Plataforma de Governança e Maturidade em Cibersegurança	Un	01
2	Assessment	Un	8.760
3	Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede)	Un	10.000
4	Serviço de Setup/Implantação	Serviço Único	01
5	Serviço de Suporte/Manutenção e Serviço Mensal	Serviço Mensal	12
6	Serviço de Transferência de Conhecimento (*Hands On*) para turmas de até 10 alunos	Turma	02

5.2. Requisitos de Negócio

5.2.1. A PRODESP conta com uma infraestrutura computacional que visa garantir o cumprimento de sua missão institucional e atender às necessidades de tecnologia da informação e comunicação das diversas unidades organizacionais em clientes externos no Estado de São Paulo.

5.2.2. As necessidades de negócio / requisitos do negócio, são metas de mais alto nível, objetivos ou necessidades da organização descritas em seu Planejamento Estratégico -2024-2028. Descrevem os itens e as razões do planejamento definido para o período, seus objetivos que devem ser atingidos e as métricas que serão utilizadas para medir o seu sucesso. Nesse

sentido , o presente item visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequada a tais objetivos estratégicos , conforme relação a seguir:

a) Atender às demandas registradas no PDTIC relacionadas à aquisição de melhoria da infraestrutura computacional ; e

b) Prover recursos computacionais necessários ao perfeito desenvolvimento das atividades que envolvem segurança da informação, em relação aos recursos de hardware e software que provenham apoio à execução das atividades da PRODESP relacionadas ao alcance junto aos seus clientes.

5.2.3. A presente contratação orienta-se pelos seguintes requisitos de negócio

5.2.3.1. Implantar uma plataforma de Governança e Maturidade em Cibersegurança:

a) Disponibilizar ambiente unificado para identificação, avaliação, classificação e priorização de riscos tecnológicos e corporativos.

b) Oferecer dashboards executivos e relatórios detalhados para subsidiar decisões estratégicas
e operacionais.

c) Mapa de controles por tipo domínio (Governança, Identificação, Proteção, Detecção, Resposta e Recuperação).

d) Uso para escolha do melhor framework e quais controles por Indicador global ou de desempenho

5.2.4. Monitorar a maturidade em segurança cibernética:

a) Estabelecer indicadores e métricas que permitam mensurar a evolução do nível de maturidade organizacional em segurança da informação.

b) Acompanhar planos de ação e evidenciar resultados em auditorias internas e externas.

c) Definição de indicadores de risco

d) Nível de exposição a vulnerabilidades críticas, severa e moderada, com ponderação por criticidade e relação de risco com o CVSS (*Common Vulnerability Scoring System*)

e) NIST CSF v2: Níveis *Partial* (1) a *Adaptive* (5).

f) CMMI aplicado à segurança: níveis de 1 (Inicial) a 5 (Otimizado).

g) CIS *Controls Implementation Groups* (IG1-IG3): progressão da adoção de controles básicos até avançados.

5.2.5. Suporte Técnico e Garantia:

a) Suporte técnico 8 (oito) horas por dia, 5 (cinco) dias por semana.

b) Atualizações de software conforme lançamentos, novos recursos, evoluções tecnológicas e correções de bugs e vulnerabilidades pelo fabricante.

5.2.6. Continuidade Operacional:

a) Mesmo após o término da garantia, os recursos e funcionalidades deverão permanecer operacionais, permitindo configurações pelos administradores.

b) Para softwares com licenciamento por subscrição, a manutenção das funcionalidades deverão ser realizadas através da renovação anual dos itens de

atualização, subscrição, manutenção e suporte técnico.

5.2.7. Atendimento Institucional:

a) Prover à PRODESP os bens de TI necessários para o atendimento institucional.

b) Prover recursos que garantam melhor rendimento, eficiência e segurança na realização das atividades institucionais.

c) Prover condições tecnológicas necessárias para prestar atendimento de qualidade aos usuários finais.

5.2.8. Disponibilidade e Performance:

a) Garantir a disponibilidade dos serviços de TI demandados pelos usuários da PRODESP.

b) Recursos que assegurem a performance adequada para acesso aos dados, informações e sistemas.

5.2.9. Segurança Cibernética:

a) Estabelecer indicadores e métricas que permitam mensurar a evolução do nível de maturidade organizacional em segurança da informação.

b) Reduzir custos e tempo despendidos em auditorias tradicionais.

c) Aplicar inteligência artificial à cibersegurança.

d) Prover mecanismos que elevem o nível de segurança cibernética e protejam os sistemas desenvolvidos e administrados pela PRODESP

5.2.10. Impacto Mínimo na Disponibilidade:

a) Assegurar que a implantação da solução cause o menor impacto possível na disponibilidade dos serviços mantidos pela PRODESP.

5.2.11. Conformidade e Continuidade dos Negócios:

a) Prover maior conformidade com regulamentações de segurança e privacidade de dados.

b) Possibilitar a continuidade dos negócios, prevenindo interrupções operacionais causadas por incidentes de segurança.

5.2.12. Redução de Custos e Riscos:

a) Diminuir custos associados à gestão de incidentes de segurança e violações.

b) Automatizar auditorias e relatórios de conformidade.

c) Fortalecer a governança de privacidade e proteção de dados.

d) Monitorar a maturidade em segurança cibernética.

5.2.13. Proporcionar a continuidade do fornecimento dos licenciamentos necessários para a manutenção e expansão das soluções utilizadas pela PRODESP e seus Clientes.

5.2.14. Viabilizar a simplificação de operações de TI, com a agilidade e flexibilidade na contratação.

5.2.15. Atender à demanda crescente dos serviços de TI pelo fornecimento de produtos e soluções.

5.2.16. Fornecer os recursos de provisionamento, integração, disponibilidade, flexibilidade,

gerenciamento, centralizado, segurança da informação, mantendo a disponibilidade dos serviços em quantidade e qualidade desejada.

5.2.17. A CONTRATADA, será responsável, fim-a-fim, por intermediar, entregar, demonstrar, gerenciar, recolher todos impostos e apoiar as aquisições da Prodesp junto aos seus clientes.

5.2.18. Deverão ser cumpridas todas as regras e políticas definidas no Termo de Contratação (e termos posteriores) firmado com a PRODESP, desde que NÃO CONFRONTEM com o estabelecido neste termo de referência

5.3. Requisitos de Capacitação

5.3.1. O Repasse de Conhecimento de que trata este Termo de Referência, refere-se a um produto de capacitação que poderá ser disponibilizado pela CONTRATADA, através de Transferência de Conhecimento (*Hands On*), conforme disposto no item 6.2 deste Termo de Referência e por intermédio de solicitação da PRODESP.

5.4. Requisitos Legais

5.4.1. Lei n.º 13.303/2016: Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

5.4.2. Regulamento Interno de Licitações e Contratos Prodesp - 2024.

5.4.3. Lei Nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD).

5.5. Requisitos de Manutenção e Suporte Técnico

5.5.1. A CONTRATADA deverá cumprir com os termos e condições de suporte técnico determinados pelo Fabricante, desde que não conflitem com as condições estipuladas neste Termo de Referência.

5.5.2. A CONTRATADA deverá disponibilizar serviço de suporte técnico via telefone, chat ou e-mail, para sanar problemas e dúvidas relativos à instalação, configuração, mudanças de topologia e demais ações que possam vir a serem executadas com os produtos especificados neste documento.

5.5.3. Deverá ser disponibilizado para a PRODESP um canal de comunicação para registros de aberturas de chamados técnicos e controles de atendimento. Os chamados serão efetuados através de telefone ou e-mail, em idioma Português-Brasil.

5.5.4. O período de disponibilidade para abertura de chamados deverá ser de 08 (oito) horas por dia, 5 (cinco) dias por semana, incluindo a capacidade de solicitar serviços online, sem limites de acionamentos aos incidentes.

5.5.5. Para os serviços de Suporte Técnico, a PRODESP poderá abrir número ilimitado de chamados durante a vigência do contrato, sem qualquer ônus adicional.

5.5.6. As manutenções e o suporte técnico sobrevivem pelo tempo contratado.

5.5.7. Caso os produtos e serviços contratados sejam processados em nuvem do próprio Fabricante, a disponibilidade dos serviços e aplicações deverá ser de, no mínimo, 99,96%.

5.5.7.1. Nos casos de disponibilidade superior ao limite mínimo estabelecido no item 5.5.7, fornecidos pelo fabricante a título de *Service Level Agreement* – SLA (Acordo de Nível de Serviço), deverá prevalecer o cenário mais vantajoso para a PRODESP, o maior nível.

5.5.8. O suporte técnico deverá atender aos seguintes itens:

- **Atendimento a Incidentes:** Suporte ágil para resolução de problemas técnicos, erros ou falhas na plataforma, com tempos de resposta definidos em SLA

(*Service Level Agreement*).

- **Dúvidas e Orientações de Uso:** Esclarecimento de dúvidas sobre as funcionalidades da plataforma, auxílio na interpretação de relatórios e orientações para o uso otimizado dos recursos.
- **Canais de Comunicação:** Disponibilidade de canal de suporte via telefone ou e-mail para facilitar a comunicação e agilizar o atendimento.
- **Atualizações de Software:** Garantia de que a plataforma esteja sempre com as versões mais recentes, incluindo correções de bugs, melhorias de desempenho e novas funcionalidades.
- **Ajustes e Otimizações:** Realização de ajustes e otimizações na configuração da plataforma para assegurar que ela opere com máxima eficiência e performance, adaptando-se às necessidades da sua infraestrutura.
- **Gestão de Integrações:** Manutenção das integrações com outras ferramentas de segurança da informação, garantindo que o fluxo de dados e informações seja contínuo e sem interrupções.
- **Melhoria Contínua:** A plataforma deve evoluir para incorporar novas tecnologias e atender às futuras demandas do mercado de segurança da informação.
- **Verificação de Saúde:** Monitoramento proativo da saúde e integridade dos componentes da plataforma, identificando potenciais gargalos ou falhas antes que impactem a operação.
- **Otimização de Banco de Dados:** Manutenção e otimização do banco de dados da plataforma para garantir a agilidade na recuperação e análise das informações de risco e conformidade.

5.5.9. Para o atendimento de chamados técnicos relacionados a sistemas/serviços ofertados pela CONTRATADA deverão ser respeitados os prazos de atendimento conforme tabela abaixo:

SLA – *Service Level Aggrement* – Nível de Serviço Aceito

Nível de Severidade	Tipo de Severidade	Descrição do Evento	Tempo para início de atendimento	Tempo para Resposta e Solução a partir do acionamento

Severidade 1 (Crítico)	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 **PRODESP** alocará um contato durante este período, seja no local ou por telefone, para auxiliar na coleta de dados, testes e aplicação de correções.	01 hora	04 horas (horário comercial)
Severidade 2 (Importante)	Alta	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 PRODESP não consegue prosseguir com a instalação de qualquer produto contratado, impedindo-o de disponibilizá-lo aos usuários.	02 horas	08 horas (Horário comercial)
Severidade 3 (Menor)	Média	A perda do serviço é pequena, o problema gera inconvenientes que podem exigir uma solução alternativa para restaurar a funcionalidade.	24 horas	48 horas (Horário comercial)
Severidade 4 (Leve)	Baixa	Não há impacto na operação e perda de serviço. O resultado não impede o funcionamento do sistema.	48 horas	72 horas (Horário comercial)

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

5.5.11. A CONTRATADA envidará esforços contínuos para solucionar as Solicitações de Serviços de Severidades 1 e 2.

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

5.5.13. A CONTRATADA priorizará o reparo de defeitos dos programas envolvidos durante a resolução das solicitações de serviço.

5.6. Ativação e uso dos produtos e serviços

5.6.1. Não se aplica para o objeto da presente contratação.

5.7. Requisitos Temporais

5.7.1. Todas as subscrições e serviços necessários à implantação e entrada em funcionamento da Plataforma, devem ser disponibilizados conforme os prazos estabelecidos neste Termo de Referência.

5.7.2. Os prazos para início da Transferência de Conhecimento (*Hands On*) devem ser definidos mediante acordo entre as partes.

5.8. Requisitos de Segurança da Informação e Privacidade

5.8.1. A CONTRATADA deverá observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação da PRODESP, inclusive sua Política de Segurança da Informação e Privacidade e Política Governança em privacidade e proteção de dados pessoais.

5.9. Requisitos Sociais e Ambientais

5.9.1. Quanto a critérios sociais, todos os profissionais da CONTRATADA que desempenharão as atividades em contato direto com a PRODESP ou seus clientes deverão cumprir os seguintes requisitos:

a) apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da PRODESP ou que ofenda o senso comum de moral e bons costumes;

b) respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;

c) atuar no estabelecimento da PRODESP com urbanidade e cortesia.

5.9.2. Quanto aos critérios ambientais, a CONTRATADA deverá cumprir os seguintes requisitos de uso racional de recursos:

a) Deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política de Nacional de Resíduos Sólidos (Lei n.º 12.305, de 2 de agosto de 2010);

b) Deverá observar entre outros: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e

obras, em consonância com o disposto no §2 do art. 27 da Lei n.º 13.303/2016.

5.10. Requisitos de Arquitetura Tecnológica

5.10.1. Não se aplica para o objeto da presente contratação.

5.11. Requisitos de Garantia e Assistência Técnica

5.11.1. As licenças deverão ser entregues acompanhadas de garantias do Fabricante e direito de atualização das versões pelo período contratado, a contar da data de entrega e ativação dos produtos e/ou serviços especificados no Contrato, minimamente:

a) A CONTRATADA deve garantir que todas as atualizações de software e patches lançados pelo fabricante sejam prontamente disponibilizados aos usuários finais. Isso inclui a implementação de medidas para garantir que os sistemas estejam sempre atualizados e protegidos contra vulnerabilidades de segurança. Entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado. Cada novo release, versão de firmware, atualização de produtos que sejam relacionados aos itens do objeto deverá ser disponibilizada pela CONTRATADA sem ônus adicional.

b) Garantir a atualização em casos de mudanças fiscais, legais e normativas pertinentes aos programas, em tempo de cumprir os prazos de entrega fixados pela legislação.

c) Atualização de versão e documentação.

d) Em caso de lançamento de novas versões, deverão ser disponibilizados à PRODESP as versões dos programas licenciados dentro do prazo de 10 (dez) dias de seu recebimento no Brasil para download, sem ônus adicional.

e) Caso, durante o período de vigência da subscrição contratada, o Fabricante desenvolva uma nova geração ou versão dos Programas Licenciados (“Novo Produto”), quer para serem utilizados com um sistema operacional ainda não desenvolvido ou com uma nova versão de um sistema operacional, esse Novo Produto será automaticamente incorporado na presente Licença. O Novo Produto deverá ser utilizado durante o prazo e de acordo com os termos do presente, sem qualquer custo adicional para a PRODESP, sendo mantida a equivalência do licenciamento contratado.

f) A PRODESP poderá, a seu critério, definir data específica para ativação dos programas contratados. Quando ocorrer, o período de garantia, o direito de atualização e o suporte técnico contratados iniciarão a partir desta data.

g) A critério da PRODESP, poderá ser requerido Manuais Técnicos e outros documentos pertinentes aos produtos contratados, em mídia digital. Neste caso, a CONTRATADA deverá entregar os arquivos no e-mail: certificados_software@prodesp.sp.gov.br.

5.12. Requisitos de Experiência Profissional

5.12.1. Não se aplica para o objeto da presente contratação.

5.12.2. Requisitos de Formação de Equipe

5.12.3. Para a execução dos serviços especificados neste Termo de Referência, a CONTRATADA deverá apresentar sua equipe de trabalho, composta pelo Gestor do Projeto e sua Equipe Técnica, na data da 1ª reunião de acompanhamento da execução do contrato **(Kickoff) entre a PRODESP e a CONTRATADA.**

5.12.4. A equipe técnica que irá executar a instalação deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de instalação (Gestor do Projeto).

5.12.5. A CONTRATADA deverá manter, durante a fase de instalação, a equipe técnica disponível para eventuais serviços executados fora do horário de expediente sem ônus adicional para a PRODESP, quando necessário para as atividades definidas no RELATÓRIO DE PROJETO DE INSTALAÇÃO e solicitado pela equipe da PRODESP.

5.12.6. A falta da execução completa de um ou mais serviços constitui-se em motivo de suspensão do compromisso financeiro, vinculados ao serviço correspondente, enquanto perdurar a ocorrência;

5.12.7. Requisitos de Metodologia de Trabalho

5.12.8. As contratações dos Produtos e Serviços, objeto do presente certame, serão realizadas conforme cessões de direito de uso da Fabricante, nas condições estipuladas neste Termo de Referência e no Contrato a ser formalizado.

5.12.9. Deverão ser cumpridas as regras e políticas definidas pelo fabricante e o Contrato, desde que não conflitem com o estabelecido neste Termo de Referência.

5.12.10. A CONTRATADA deverá prover todas as condições necessárias junto ao Fabricante para a PRODESP obter acesso aos serviços de contratados.

5.12.11. Para os recursos contratados e suas atualizações, a CONTRATADA deverá fornecer todas as informações necessárias e o apoio a PRODESP, para o processo de instalação, configuração, transferência de dados e uso dos recursos (licenças de software, servidores, storage, backup etc).

5.13. Requisitos Técnicos

- A plataforma deverá rodar na modalidade de SaaS e ficar hospedada no ambiente da CONTRATADA.
- A plataforma deverá possuir licenciamento específicos para software de governança, maturidade e avaliação de segurança da informação, modulo de assessment e devices sendo disponibilizadas de acordo com a tabela de quantidades especificada neste termo de referência.
- A plataforma deverá possuir controle de acessos, com níveis diferenciados para administrador.
- A plataforma deverá ter os inventários dos ativos, assim como o apontamento dos Ativos Críticos ao Negócio ou Serviços a fim de manter a avaliação continuada de risco.

5.13.1. A Plataforma de Governança e Maturidade em Cibersegurança é uma plataforma de software único, destinada à gestão de maturidade cibernética e corporativa, deverá também em sua arquitetura, ser uma solução única, coesa e integral, não se tratando de um conjunto de sistemas distintos, ainda que integrados, de diferentes fabricantes.

5.13.2. Qualquer proposta que utilize a integração de múltiplos softwares, produtos ou plataformas do mesmo fabricante ou de terceiros para atender aos requisitos técnicos e funcionais deste Termo de Referência será desclassificada, uma vez que a solução deve ser concebida e fornecida como uma única plataforma por um único fabricante, visando a eficácia operacional, a segurança e a simplificação do suporte e da manutenção.

5.14. Requisitos Técnicos da Plataforma

5.14.1. A plataforma deverá suportar e atender obrigatoriamente as tecnologias abaixo:

5.14.1.1. Arquitetura e Tecnologias

a) Front-end: A interface do usuário (UI) da plataforma deverá ser por meio de um SaaS, garantindo uma experiência de usuário (UX) moderna, responsiva,

interativa e de alta performance.

b) Back-end: A plataforma deverá possuir API RESTfull escalável, eficiente e de alto desempenho, capaz de suportar um grande volume de requisições e processamento de dados. A API deve ser bem documentada (Swagger) e seguir princípios de segurança como autenticação, validação de entradas e proteção contra vulnerabilidades comuns.

c) Banco de Dados: O banco de dados deverá ser projetado com alta performance, com índices adequados, procedures otimizadas e um esquema de banco de dados robusto que garanta a integridade e consistência dos dados.

d) Infraestrutura de Hospedagem: Toda a infraestrutura da plataforma (*front-end*, *back-end* e banco de dados) deverá ser hospedada no modelo SaaS.

I - Requisitos de Infraestrutura e Desempenho SaaS.

- Ambiente SaaS de alta performance no Brasil;
- Redundância de Zonas de Disponibilidade (Availability Zones) para alta resiliência, deve ser projetada para garantir alta disponibilidade, utilizando recursos como com múltiplos nós e balanceamento de carga com opções de redundância geográfica e *failover* automático.
- Armazenamento com criptografia AES-256;
- Banco de Dados, deverá ser relacional, suportar Linguagem T-SQL, ter segurança avançada com Criptografia de dados em repouso e em trânsito e controle de acesso baseado em funções (RBAC).
- SLA (*Service Level Agreement*): A solução deverá garantir um SLA de 99,96% de disponibilidade para a plataforma como um todo, conforme os SLAs oferecidos pelos serviços do Cloud de mercado.
- Escalabilidade: A plataforma deve ser escalável horizontal e verticalmente para acomodar o crescimento futuro do volume de dados e do número de usuários, utilizando os recursos de auto escalabilidade do Serviços de Cloud.

II - Segurança da Infraestrutura: Serão implementadas as melhores práticas de segurança no modelo SaaS, incluindo:

- Rede Virtual (VNet): Isolamento da rede da aplicação e banco de dados.
- Grupos de Segurança de Rede (NSG): Controle de tráfego de entrada e saída.
- Gerenciamento seguro de chaves, segredos e certificados.
- Integração para autenticação e autorização
- Monitoramento de Segurança para detecção de ameaças e auditoria.
- Backups e Restauração: Configuração de políticas de backup e recuperação de desastres para banco de dados e aplicações.
- Firewall: Configuração de firewall para o banco de dados e aplicações, permitindo acesso apenas de IPs autorizados.

- Gerenciamento Simplificado: A utilização dos serviços gerenciados deve proporcionar um gerenciamento simplificado da infraestrutura, reduzindo a complexidade operacional.

III - Usabilidade (*User Experience* - UX)

- A plataforma deverá dispor de uma interface de usuário (UI) moderna, intuitiva e de fácil navegação, projetada para otimizar a experiência de administradores e usuários.

- Design Responsivo: A interface deve ser plenamente responsiva, adaptando-se a diferentes tamanhos de tela (*desktops, notebooks, tablets*), sem perda de funcionalidade ou clareza visual.

- Visão Centralizada: Deverá oferecer dashboards personalizáveis e painéis de controle que apresentem as informações de risco, conformidade e maturidade de forma clara e consolidada, utilizando gráficos, *widgets* e indicadores de desempenho (KPIs).

- Acesso Baseado em Perfis (RBAC): A solução deve implementar um controle de acesso baseado em papéis (*Role-Based Access Control* - RBAC), permitindo a concessão de diferentes níveis de permissão (administrador, operador, visualizador) para garantir que cada usuário visualize apenas as informações e funcionalidades pertinentes ao seu perfil.

IV - Performance

- A plataforma deverá garantir alto desempenho, escalabilidade e resiliência, independentemente do volume de dados, número de usuários e complexidade das operações.

- Tempo de Resposta: Todas as funcionalidades críticas, como a geração de relatórios de risco, a análise de conformidade e a navegação entre os módulos, deverão apresentar tempos de resposta inferiores a 5 (cinco) segundos.

- Escalabilidade: A arquitetura da solução deve ser escalável horizontalmente e verticalmente, permitindo o acréscimo de recursos (CPU, memória, armazenamento) para suportar o crescimento futuro do volume de dados e o aumento da carga de trabalho, sem comprometer a performance.

- Processamento de Dados: A plataforma deverá ser capaz de processar e analisar grandes volumes de dados de segurança da informação (big data), provenientes de diferentes fontes (ferramentas de segurança, logs, etc.), de forma eficiente e sem degradação perceptível de desempenho.

V - Segurança da Aplicação

- A plataforma deverá ser desenvolvida e mantida com foco rigoroso em segurança, mitigando os riscos de vulnerabilidades na própria aplicação.

- Padrões de Segurança: O código da aplicação deve seguir as melhores práticas de segurança, em conformidade com o OWASP Top 10, incluindo a validação robusta de todas as entradas de dados, para prevenir ataques.

- Proteção Contra Ameaças: A solução deve ser intrinsecamente protegida

contra as ameaças de segurança mais comuns, tais como:

- SQL *Injection*: Prevenção de injeções de código SQL através de consultas parametrizadas e sanitização de entradas.
- *Cross-Site Scripting* (XSS): Proteção contra a injeção de scripts maliciosos em páginas web.
- *Cross-Site Request Forgery* (CSRF): Mecanismos para garantir que as requisições de usuário sejam legítimas e não forjadas.
- Criptografia: Todos os dados sensíveis, em repouso e em trânsito, deverão ser criptografados usando algoritmos robustos e amplamente aceitos, como AES-256 para dados em repouso e TLS 1.2 ou superior para dados em trânsito.

VI - Compatibilidade

- A plataforma deverá ser compatível com os principais navegadores de internet utilizados pelo Órgão, garantindo a acessibilidade e a funcionalidade para todos os usuários.
- Navegadores: A solução deverá ser totalmente funcional e compatível, no mínimo, com as versões mais recentes dos navegadores Google Chrome, Mozilla Firefox e Microsoft Edge, sem a necessidade de plugins ou extensões de terceiros.
- A plataforma deverá ter controles por função de atuação com as quantidades correlacionadas diretamente com os demais frameworks, melhores práticas, regulamentos, métodos e leis:
- *Govern* (GV) – Governança da cibersegurança – mínimo 213 controles
- *Identify* (ID) – Inventário e gestão de ativos – mínimo 197 controles
- *Protect* (PR) – Implementação de medidas de proteção – mínimo 368
- *Detect* (DE) – Capacidade de identificar incidentes – mínimo 62
- *Respond* (RS) – Resposta a incidentes – mínimo 54
- *Recover* (RC) – Continuidade e recuperação – mínimo 23

VII - Funcionalidades do Software

- A plataforma a ser contratada deverá contemplar, obrigatoriamente, os seguintes requisitos técnicos mínimos, observando padrões internacionais, melhores práticas, métodos reconhecidos e legislações nacionais e internacionais:

a) NIST Cybersecurity Framework (CSF)

- *Organizational Context* (GV.OC)
- *Risk Management Strategy* (GV.RM)
- *Roles, Responsibilities, and Authorities* (GV.RR)

- *Policy* (GV.PO)
- *Oversight* (GV.OV)
- *Cybersecurity Supply Chain Risk Management* (GV.SC)
- *Asset Management* (ID.AM)
- *Risk Assessment* (ID.RA)
- *Improvement* (ID.IM)
- *Identity Management, Authentication, and Access Control* (PR.AA)
- *Awareness and Training* (PR.AT)
- *Data Security* (PR.DS)
- *Platform Security* (PR.PS)
- *Technology Infrastructure Resilience* (PR.IR)
- *Continuous Monitoring* (DE.CM)
- *Adverse Event Analysis* (DE.AE)
- *Incident Management* (RS.MA)
- *Incident Analysis* (RS.AN)
- *Incident Response Reporting and Communication* (RS.CO)
- *Incident Mitigation* (RS.MI)
- *Incident Recovery Plan Execution* (RC.RP)
- *Incident Recovery Communication* (RC.CO)

b) NIST *Cybersecurity Framework* (CSF) SP 800

c) NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*)

- Definir escopo e limites da avaliação
- Selecionar modelo de risco e critérios
- Identificar ameaças
- Identificar vulnerabilidades
- Determinar probabilidade
- Estimar impacto
- Determinar risco (nível)
- Documentar cenários de risco
- Analisar incerteza

- Recomendar respostas ao risco
- Registrar no *Risk Register*
- Comunicar resultados
- Integração com ciclo de mudanças
- Critérios de aceitação de risco
- Monitoramento contínuo de risco
- Validação e QA da avaliação
- Integração com BIA e continuidade
- Mapeamento a controles existentes
- Priorização baseada em valor

d) NIST SP 800-12 - Introdução à Segurança da Informação

- Política de Segurança da Informação
- Programa de Conscientização e Treinamento
- Gestão de Acessos e Identidades
- Proteção de Dados
- Gestão de Configuração Segura
- Gestão de Vulnerabilidades
- Monitoramento e Logs
- Resposta a Incidentes
- Contingência e Recuperação
- Criptografia
- Segurança de Redes
- Segurança Física e Ambiental
- Segurança de Aplicações
- Gestão de Provedores/Fornecedores

e) NIST SP 800-39 - Gestão de Riscos Organizacionais

- *Framing* do Risco (Contextualização)
- Governança de Risco (*Risk Executive*)
- Integração Risco e Missão
- *Tiering* Organizacional

- Integração com SDLC e Aquisições
- *Risk Assessment* recorrente
- *Risk Response*
- *Risk Monitoring*
- Relato Executivo e Conformidade
- Risco de Terceiros e *Supply Chain*
- Cultura e Apetite a Risco

f) NIST SP 800-88 - Sanitização de Mídias

- Política de Sanitização
- Inventário de Mídias
- Classificação dos Dados
- Matriz de Decisão de Método
- *Clear* (limpeza lógica)
- *Purge* (purga)
- *Destroy* (destruição)
- Cadeia de Custódia
- Registro e Evidências
- Verificação Independente
- Exceções e Emergências
- Considerações *Cloud*/Virtual

g) CIS *Controls* (última versão)

- Implementação dos 18 controles críticos com dashboards de conformidade.
    - CIS 1 - *Inventory and Control of Enterprise Assets*
    - CIS 2 - *Inventory and Control of Software Assets*
    - CIS 3 - *Data Protection*
    - CIS 4 - *Secure Configuration of Enterprise Assets and Software*
    - CIS 5 - *Account Management*
    - CIS 6 - *Access Control Management*
    - CIS 7 - *Continuous Vulnerability Management*
    - CIS 8 - *Audit Log Management*
    - CIS 9 - *Email and Web Browser Protections*
    - CIS 10 - *Malware Defenses*
    - CIS 11 - *Data Recovery*
    - CIS 12 - *Network Infrastructure Management*
    - CIS 13 - *Network Monitoring and Defense*
    - CIS 14 - *Security Awareness and Skills Training*

- CIS 15 - *Service Provider Management*
- CIS 16 - *Application Software Security*
- CIS 17 - *Incident Response Management*
- CIS 18 - *Penetration Testing*

h) NIST IA RMF v1

- GOVERN 1.1: Requisitos legais e regulatórios envolvendo IA são compreendidos, gerenciados e documentados.
- GOVERN 1.2: As características de IA confiável são integradas em políticas, processos, procedimentos e práticas organizacionais.
- GOVERN 1.3: Processos, procedimentos e práticas estão estabelecidos para determinar o nível necessário de atividades de gestão de risco com base na tolerância a risco da organização.
- GOVERN 1.4: O processo de gestão de risco e seus resultados são estabelecidos por meio de políticas, procedimentos e outros controles transparentes, baseados nas prioridades de risco da organização.
- GOVERN 1.5: Monitoramento contínuo e revisão periódica do processo de gestão de risco e seus resultados são planejados e papéis e responsabilidades organizacionais claramente definidos, incluindo a frequência das revisões.
- GOVERN 1.6: Mecanismos estão implementados para inventariar sistemas de IA e são alocados recursos de acordo com prioridades de risco da organização.
- GOVERN 1.7: Processos e procedimentos estão estabelecidos para descomissionamento e desativação de sistemas de IA de forma segura, sem aumentar riscos ou diminuir a confiabilidade da organização.
- GOVERN 2.1: Papéis, responsabilidades e linhas de comunicação relacionadas à gestão de riscos de IA estão documentadas e são claras para indivíduos e equipes na organização.
- GOVERN 2.2: Pessoal da organização e parceiros recebem treinamento em gestão de riscos de IA para desempenhar suas funções de acordo com políticas, procedimentos e acordos relacionados.
- GOVERN 3.1: Tomada de decisão relacionada à gestão de riscos de IA é informada por uma equipe diversificada (demografia, disciplinas, experiência, expertise, histórico).
- GOVERN 3.2: Políticas e procedimentos definem e diferenciam papéis e responsabilidades em configurações humano-IA e supervisão de sistemas de IA.
- GOVERN 4.1: Políticas e práticas organizacionais promovem pensamento crítico e mentalidade de segurança em design, desenvolvimento, implantação e uso de sistemas de IA.
- GOVERN 4.2: Equipes documentam riscos e impactos potenciais da tecnologia de IA e comunicam amplamente esses impactos.

- GOVERN 4.3: Práticas organizacionais permitem testes de IA, identificação de incidentes e compartilhamento de informações.
- GOVERN 5.1: Políticas e práticas organizacionais coletam, consideram, priorizam e integram feedback de partes externas sobre impactos individuais e sociais relacionados a riscos de IA.
- GOVERN 5.2: Mecanismos permitem que a equipe que desenvolveu ou implantou sistemas de IA incorpore regularmente feedback adjudicado de atores relevantes de IA em design e implementação.
- GOVERN 6.1: Políticas e procedimentos abordam riscos de IA associados a terceiros, incluindo violação de propriedade intelectual ou outros direitos.
- GOVERN 6.2: Processos de contingência para lidar com falhas ou incidentes em dados ou sistemas de IA de terceiros considerados de alto risco.
- MAP 1.1: Propósitos pretendidos, usos potencialmente benéficos, leis e normas contextuais, expectativas e ambientes prospectivos para sistemas de IA são compreendidos e documentados. Considera: tipos de usuários e expectativas; impactos positivos e negativos; suposições e limitações sobre propósitos, usos e riscos; métricas relacionadas.
- MAP 1.2: Atores interdisciplinares de IA, competências, habilidades e capacidades refletem diversidade demográfica, expertise ampla e participação documentada.
- MAP 1.3: Missão da organização e objetivos relevantes para tecnologia de IA são compreendidos e documentados.
- MAP 1.4: Valor ou contexto de negócio claramente definido ou reavaliado para sistemas existentes.
- MAP 1.5: Tolerâncias a risco organizacionais determinadas e documentadas.
- MAP 1.6: Requisitos do sistema (ex.: “o sistema deve respeitar a privacidade dos usuários”) são provocadas e compreendidos pelos atores de IA relevantes.
- MAP 2.1: Tarefas e métodos que o sistema de IA apoiará definidos (ex.: classificadores, modelos generativos, recomendadores).
- MAP 2.2: Limites de conhecimento do sistema de IA e supervisão humana documentados.
- MAP 2.3: Integridade científica e considerações TEVV identificadas e documentadas, incluindo design experimental, coleta de dados, confiabilidade e validação.
- MAP 3.1: Benefícios potenciais da funcionalidade e desempenho do sistema de IA examinados e documentados.
- MAP 3.2: Custos potenciais, inclusive não monetários, decorrentes de erros de IA ou funcionalidade do sistema são examinados e documentados.

- MAP 3.3: Escopo de aplicação alvo especificado e documentado com base na capacidade do sistema, contexto e categorização.
- MAP 3.4: Processos de proficiência de operadores e profissionais definidos, avaliados e documentados, incluindo padrões e certificações.
- MAP 3.5: Processos de supervisão humana definidos, avaliados e documentados conforme políticas do Governo.
- MAP 4.1: Abordagens para mapeamento de riscos tecnológicos e legais de componentes – incluindo uso de dados ou software de terceiros – implementadas e documentadas.
- MAP 4.2: Controles internos para componentes de IA incluindo tecnologias de terceiros, identificados e documentados.
- MAP 5.1: Probabilidade e magnitude de cada impacto identificado (positivo ou negativo) baseado em uso esperado, histórico, incidentes públicos, feedback de atores externos ou outros dados.
- MAP 5.2: Práticas e pessoal para engajamento regular com atores de IA e integração de feedback implementados e documentados.
- MEASURE 1.1: Abordagens e métricas para mensuração de riscos de IA selecionadas e implementadas, começando pelos riscos mais significativos. Riscos não mensuráveis são documentados.
- MEASURE 1.2: Apropriação das métricas de IA e eficácia dos controles existentes avaliadas e atualizadas regularmente.
- MEASURE 1.3: Especialistas internos não envolvidos diretamente no desenvolvimento ou avaliadores independentes participam de avaliações regulares.
- MEASURE 2.1: Conjuntos de teste, métricas e detalhes das ferramentas usadas durante TEVV documentados.
- MEASURE 2.2: Mecanismos aplicados para manter valor dos sistemas de IA implementados.
- MEASURE 2.3: Procedimentos seguidos para responder e recuperar de riscos previamente desconhecidos.
- MEASURE 2.4: Mecanismos aplicados e responsabilidades atribuídas para substituir, desativar ou descontinuar sistemas de IA que não atendam ao uso pretendido.
- MEASURE 2.5: O sistema de IA a ser implantado é demonstrado como válido e confiável. As limitações da generalização além das condições em que a tecnologia foi desenvolvida são documentadas.
- MEASURE 2.6: O sistema de IA é avaliado regularmente quanto aos riscos de segurança, conforme identificados na função MAP. O sistema de IA a ser implantado demonstra ser seguro, seu risco negativo residual não excede a tolerância ao risco e pode falhar com segurança, especialmente se for operado além dos seus limites de conhecimento. As métricas de segurança refletem a confiabilidade e a robustez do sistema, o

monitoramento em tempo real e os tempos de resposta a falhas do sistema de IA.

- MEASURE 2.7: A segurança e a resiliência do sistema de IA – conforme identificadas na função MAP – são avaliadas e documentadas.
- MEASURE 2.8: Os riscos associados à transparência e à responsabilização – conforme identificados na função MAP – são examinados e documentados.
- MEASURE 2.9: O modelo de IA é explicado, validado e documentado, e os resultados do sistema de IA são interpretados em seu contexto – conforme identificado na função MAP – para informar o uso responsável e a governança.
- MEASURE 2.10: O risco à privacidade do sistema de IA – conforme identificado na função MAP – é examinado e documentado.
- MEASURE 2.11: A imparcialidade e a parcialidade – conforme identificadas na função MAP – são avaliadas e os resultados são documentados.
- MEASURE 2.12: O impacto ambiental e a sustentabilidade das atividades de treinamento e gestão do modelo de IA – conforme identificados na função MAP – são avaliados e documentados.
- MEASURE 2.13: A eficácia das métricas e processos de TEVV (*Test, Evaluation, Verification, and Validation*) empregados na função MEASURE são avaliados e documentados.
- MEASURE 3.1: Abordagens, pessoal e documentação estão disponíveis para identificar e monitorar regularmente os riscos de IA existentes, imprevistos e emergentes, com base em fatores como o desempenho pretendido e real em contextos implementados.
- MEASURE 3.2: Abordagens de monitoramento de riscos são consideradas para cenários onde os riscos de IA são difíceis de avaliar usando as técnicas de mensuração atualmente disponíveis ou onde as métricas ainda não estão disponíveis.
- MEASURE 3.3: Os processos de feedback para usuários finais e comunidades impactadas para relatar problemas e apelar aos resultados do sistema são estabelecidos e integrados às métricas de avaliação do sistema de IA
- MEASURE 4.1: As abordagens de mensuração para identificar riscos de IA são conectadas ao(s) contexto(s) de implantação e informadas por meio de consultas com especialistas da área e outros usuários finais. As abordagens são documentadas.
- MEASURE 4.2: Os resultados das medições referentes à confiabilidade do sistema de IA no(s) contexto(s) de implantação e ao longo do ciclo de vida da IA são informados por informações de especialistas da área e de atores relevantes da IA para validar se o sistema está funcionando de forma consistente conforme o esperado. Os resultados são documentados.
- MEASURE 4.3: Melhorias ou declínios mensuráveis no desempenho, com

base em consultas com atores relevantes da IA incluindo comunidades afetadas, e dados de campo sobre riscos relevantes ao contexto e características de confiabilidade, são identificados e documentados.

- MANAGE 1.1: Determina-se se o sistema de IA atinge seus propósitos pretendidos e objetivos declarados e se seu desenvolvimento ou implantação deve prosseguir.
- MANAGE 1.2: O tratamento dos riscos de IA documentados é priorizado com base no impacto, probabilidade e recursos ou métodos disponíveis.
- MANAGE 1.3: As respostas aos riscos de IA considerados de alta prioridade, conforme identificados pela função MAP, são desenvolvidas, planejadas e documentadas. As opções de resposta aos riscos podem incluir mitigação, transferência, prevenção ou aceitação.
- MANAGE 1.4: Os riscos residuais negativos (definidos como a soma de todos os riscos não mitigados) tanto para os adquirentes a jusante dos sistemas de IA quanto para os usuários finais são documentados.
- MANAGE 2.1: Os recursos necessários para gerenciar os riscos de IA são levados em consideração – juntamente com sistemas, abordagens ou métodos alternativos não baseados em IA viáveis – para reduzir a magnitude ou a probabilidade de impactos potenciais.
- MANAGE 2.2: Mecanismos estão em vigor e são aplicados para sustentar o valor dos sistemas de IA implantados.
- MANAGE 2.3: Procedimentos são seguidos para responder e se recuperar de um risco previamente desconhecido quando ele é identificado.
- MANAGE 2.4: Mecanismos estão em vigor e são aplicados, e responsabilidades são atribuídas e compreendidas, para substituir, desengajar ou desativar sistemas de IA que demonstrem desempenho ou resultados inconsistentes com o uso pretendido.
- MANAGE 3.1: Os riscos e benefícios da IA provenientes de recursos terceirizados são monitorados regularmente, e os controles de risco são aplicados e documentados.
- MANAGE 3.2: Os modelos pré-treinados utilizados para o desenvolvimento são monitorados como parte do monitoramento e manutenção regulares do sistema de IA.
- MANAGE 4.1: Os planos de monitoramento do sistema de IA pós-implantação são implementados, incluindo mecanismos para capturar e avaliar as contribuições dos usuários e outros atores relevantes da IA, apelação e substituição, descomissionamento, resposta a incidentes, recuperação e gerenciamento de mudanças.
- MANAGE 4.2: Atividades mensuráveis para melhorias contínuas são integradas às atualizações do sistema de IA e incluem o engajamento regular com as partes interessadas, incluindo os atores relevantes da IA.
- MANAGE 4.3: Incidentes e erros são comunicados aos atores relevantes da IA incluindo as comunidades afetadas. Os processos de rastreamento,

resposta e recuperação de incidentes e erros são seguidos e documentados.

i) ISO/IEC 27001

- Gestão completa do SGSI (Sistema de Gestão da Segurança da Informação) com módulos para políticas, riscos e controles.
- Mapeamento dos controles do Anexo A, com no mínimo 34 grupos de controles, assim como ratificação das evidências ou aplicação de auditoria registrada, baseando-se na descrição da norma.

  -> A.5 - Controles Organizacionais
  -> A.6 - Controles de pessoas
  -> A.7 - Controles físicos
  -> A.8 - Controles tecnológicos

- Relatórios de conformidade compatíveis com auditorias internas e externas.
- Workflow para planos de ação corretiva, gestão de riscos e melhoria contínua.

j) ISO 27701 / LGPD (Lei 13.709/2018)

- Registro completo das operações de tratamento de dados pessoais.
- Gestão de solicitações de titulares (ex.: exclusão, portabilidade, correção de dados).
- Painel de autoatendimento para titulares exercerem seus direitos.
- Funcionalidades de anonimização, pseudonimização e minimização de dados.
- Relatórios de Impacto à Proteção de Dados (RIPD) automatizados.
- Trilhas de auditoria exportáveis para comprovação junto à ANPD e órgãos de controle.
- ISO.27701-PIM A.7.2 - Condições para coleta e tratamento
- ISO.27701-PIM A.7.3 - Obrigações para os titulares de Dados Pessoais
- ISO.27701-PIM A.7.4 - *Privacy by design* e *Privacy by Default*
- ISO.27701-PIM A.7.5 - Compartilhamento, transferência e divulgação de DP
- ISO.27701-PIM A.B.8.2 Condições para coleta e tratamento
- ISO.27701-PIM A.B.8.3 Obrigações para os titulares de DP
- ISO.27701-PIM A.B.8.4 *Privacy by design* e *Privacy by Default*
- ISO.27701-PIM A.B.8.5 Compartilhamento, transferência e descarte de DP

k) ISO 22301 *Business continuity management systems*

- ISO.22301-BC Art 5.1, 5.3 - Liderança, comprometimento e governança do

SGCN (Sistema de Gestão da Continuidade de Negócios)

- ISO.22301-BC Art 5.2 -SO.22301-BC S.5 - Política de Continuidade de Negócios
- ISO.22301-BC Art 5.3 - Estrutura organizacional, autoridade e responsabilidade
- ISO.22301-BC Art 6.1- Planejamento – riscos e oportunidades
- ISO.22301-BC Art 6.2, 9.1 - Objetivos do SGCN, monitoramento e avaliação de desempenho
- ISO.22301-BC Art 7.1, 8.1 - Recursos, infraestrutura e ambiente de operação
- ISO.22301-BC Art 7.2, 7.3- Competência, conscientização e treinamento
- ISO.22301-BC Art 7.3, 7.4- Conscientização e comunicação organizacional
- ISO.22301-BC Art 7.4, 8.4- Comunicação, planos de contingência e crises
- ISO.22301-BC Art 8.2.1, 8.2.3- Análise de Impacto nos Negócios, identificação de processos críticos
- ISO.22301-BC Art 8.2.2, 8.2.3- Avaliação de riscos de continuidade
- ISO.22301-BC Art 8.3, 8.4 - Estratégias e soluções de continuidade
- ISO.22301-BC Art 8.4.2, 8.5- Planejamento de resposta a incidentes e continuidade
- ISO.22301-BC Art 8.5.4, 10.1- Testes, exercícios e melhoria contínua
- ISO.22301-BC Art 9.1, 9.2 - Avaliação de desempenho, auditorias internas
- ISO.22301-BC Art 10.1, 10.2 - Melhoria contínua, ações corretivas e preventivas

l) ISO/IEC 27005 – Gestão de Riscos de Segurança da Informação

- A ISO/IEC 27005:2022 é a norma que fornece diretrizes para a gestão de riscos em segurança da informação, sendo complementar à ISO/IEC 27001.
- "Adoção de abordagem quantitativa.
- Adoção de escalas de consequências, como exemplo: 1 – Menor, 2 – Significativa, 3 – Séria, 4 – Crítica, 5 – Catastrófica.
- Adoção de escalas probabilidade, como exemplo: 1 – Improvável, 2 – Bastante improvável, 3 – Provável, 4 – Muito provável e 5 – Quase certo.
- Emprego de uma matriz com Probabilidade e Consequência com visão qualitativa"
- Os critérios para a aceitação do risco podem ser simplesmente um valor acima do qual os riscos são considerados inaceitáveis. Utiliza-se uma

matriz de risco codificada por cores, espelhando as escalas para consequência e probabilidade, as organizações podem apresentar graficamente a distribuição de risco de uma ou várias avaliações de risco. Esta matriz de risco também pode ser utilizada para sinalizar a atitude da organização com relação aos valores de risco, e indicar se convém que um risco seja normalmente aceito ou tratado. Ex.: Baixo (verde) = Aceitável como é apresentado, Moderado (amarelo) = Tolerável sob controle e Alto (vermelho) = Inaceitável

- Ao identificar e avaliar os riscos de segurança da informação, convém que sejam levados em conta os seguintes exemplos: eventos de segurança e incidentes (dentro e fora da organização); fontes de risco; vulnerabilidades exploradas; consequências medidas; ameaças; vulnerabilidades; consequências; cenários de risco.

- No processo de tratamento de riscos, cada controle é aplicável a um subconjunto dos ativos. Os ativos podem ser divididos em duas categorias: ativos primários/de negócio; informações ou processos de valor para uma organização; ativos de suporte – componentes do sistema de informações em que um ou vários ativos de negócios estão fundamentados.

- "Pode-se adotar propõe caracterizar alguns tipos de fontes de risco. Dois critérios principais estruturam essa abordagem descritiva: a motivação e a capacidade de agir.

- Sugere-se que haja entendimento das ameaças. Embora não seja possível expressar diretamente uma motivação, ela pode ser apresentada por meio da intenção da fonte de risco e expressa na forma de um estado final desejado (*Desired End State* - DES): a situação geral que a fonte de risco quer alcançar após o confronto"

- Em uma abordagem com base em eventos, convém que os cenários sejam construídos analisando os diferentes caminhos, relevantes para as interações entre a organização e as partes interessadas, que formam um ecossistema que as fontes de risco podem usar para alcançar os ativos do negócio e seus DES. As partes interessadas no escopo do SGSI que convém que sejam consideradas ao analisar cenários de risco, podem ser de dois tipos: partes externas, incluindo: clientes; sócios, cocontratantes; prestadores de serviços (subcontratados, fornecedores) e partes internas, incluindo: prestadores de serviços técnicos (por exemplo, serviços de suporte propostos pela gestão de TI);prestadores de serviços de negócios (por exemplo, entidade comercial que utiliza dados de negócios); subsidiárias (em particular, localizadas em outros países).

- "Ameaças consideradas como fontes de risco podem ser deliberadas, como acidentais ou ambientais (naturais) e podem resultar, por exemplo, em danos ou perda de serviços essenciais. A lista indica para cada tipo de ameaça onde D (deliberada), A (acidental), E (ambiental) é relevante. Sugere-se a categorização das Ameaças: Ameaças físicas, Ameaças naturais, Falhas na infraestrutura, Falhas técnicas, Ações humanas, Comprometimento de funções ou serviços, Ameaças organizacionais etc. Já a tabela de vulnerabilidades, pode-se categorizar com por tipos: Hardware, Software, Rede/Cloud, Pessoal, Local, Organizacional. "

- Os cenários de risco podem ser construídos usando uma abordagem

baseada em eventos, uma abordagem baseada em ativos ou ambos. A matriz com Fonte de risco vs Objetivo de alvo DES vs Cenário estratégico de risco (base em eventos) vs Cenário de risco operacional (ativos).

- O monitoramento de eventos relacionados ao risco é a identificação de fatores que podem influenciar um cenário de risco de segurança da informação.

m)ISO 23894 - *Artificial intelligence*: fornece orientações para identificar, analisar, avaliar e tratar riscos relacionados ao uso de IA.

- ISO.23894-AI-A.1 - Generalidades: Ao identificar os riscos dos sistemas de IA
- ISO.23894-AI-A.2 - Responsabilização A responsabilização refere-se tanto a uma característica das organizações quanto a uma propriedade do sistema.
- A.3 - Experiência em IA - Os sistemas de IA e seu desenvolvimento são diferentes das soluções de software não IA
- ISO.23894-AI-A.4 - Disponibilidade e qualidade dos dados de treinamento e teste
- ISO.23894-AI-A.5 - Impacto ambiental - O uso da IA pode causar efeitos do ponto de vista ambiental.
- ISO.23894-AI-A.6 - Justiça - O uso de sistemas de IA para a tomada de decisões automatizadas pode ser injusto para pessoas ou grupos de pessoas específicas
- ISO.23894-AI-A.7 - Manutenibilidade - A manutenibilidade está relacionada à capacidade da organização de lidar com modificações no sistema de IA, a fim de corrigir defeitos ou ajustar-se aos novos requisitos
- ISO.23894-AI-A.8 - Privacidade - A privacidade está relacionada à capacidade dos indivíduos de controlar ou influenciar quais informações relacionadas a eles podem ser coletadas, armazenadas e processadas, e por quem essas informações podem ser divulgadas.
- ISO.23894-AI-A.9 Robustez - A robustez está relacionada à capacidade de um sistema de manter seu nível de desempenho sob as várias circunstâncias de seu uso
- ISO AI-A.10 Segurança física (*safety*) - O uso de sistemas de IA pode introduzir novas ameaças à segurança física. A segurança física refere-se à expectativa de que um sistema não conduza, em condições definidas, a um estado em que a vida, a saúde, a propriedade ou o ambiente humano estejam em perigo.
- ISO.23894-AI-A.11 Segurança (*security*) - A gestão de riscos de segurança da informação é definida na ABNT NBR ISO/IEC 27005:2023
- ISO.23894-AI-A.12 - Transparência e explicabilidade - A transparência está relacionada tanto às características de uma organização que opera sistemas de IA quanto aos próprios sistemas.

- ISO.23894-AI-B.1 Generalidades - Ao identificar os riscos dos sistemas de IA, convém que sejam levadas em conta as várias fontes de riscos, dependendo da natureza do sistema em consideração e do seu contexto de aplicação.

- ISO.23894-AI-B.2 - Complexidade do ambiente - A complexidade do ambiente de um sistema de IA determina a gama de situações potenciais que um sistema de IA se destina a suportar no seu contexto operacional.

- ISO.23894-AI-B.3 Falta de transparência e explicabilidade - Transparência é sobre a comunicação de atividades e decisões apropriadas de uma organização

- ISO.23894-AI-B.4 - Nível de automação os sistemas de IA podem operar com diferentes níveis de automação.

- ISO.23894-AI-B.5 - Fontes de riscos relacionadas ao aprendizado de máquina.

- ISO.23894-AI-B.6 - Problemas de hardware do sistema. As fontes de riscos relacionadas aos problemas de hardware

- ISO.23894-AI-B.7 Problemas do ciclo de vida do sistema e métodos, processos e o uso inadequado ou insuficiente de um sistema de IA ao longo de seu ciclo de vida podem levar a riscos.

- ISO.23894-AI-B.8 - Prontidão tecnológica indica o quão madura uma determinada tecnologia está em um determinado contexto de aplicação.

VIII - Avaliação de Uso de Tecnologias e Ferramentas de Segurança da Informação

- Os requisitos técnicos para a plataforma no que diz respeito à avaliação e ao mapeamento das tecnologias de segurança da informação da CONTRATANTE, com base nas fases do ciclo de segurança cibernética.

IX - Mapeamento e Análise Tecnológica

- A plataforma deverá ser capaz de mapear e analisar as tecnologias de segurança da informação (SIEM, EDR/XDR, DLP, entre outras) utilizadas pela CONTRATANTE. Essa análise deve ser correlacionada com as seguintes fases do ciclo de segurança cibernética:

    - Governança: Avaliação de ferramentas que auxiliam na gestão de riscos, na definição de políticas e na conformidade com regulamentações.

    - Identidade: Análise de tecnologias de gestão de identidade e acesso (IAM, PAM), controle de acesso à rede (NAC) e autenticação multifator (MFA).

    - Proteção: Avaliação de soluções que previnem ataques (Firewall, WAF, Proteção de E-mail, Segurança de *Endpoint*) e que protegem dados e infraestrutura.

    - Detecção de Ameaças: Análise de ferramentas que identificam atividades maliciosas (NDR, EDR/XDR, SIEM, Gerenciamento de

Vulnerabilidades) e que monitoram o ambiente de forma contínua.

- Resposta a Incidentes: Avaliação de tecnologias que auxiliam na contenção, erradicação e recuperação de incidentes (EDR/XDR).

- Recuperação: Análise de soluções que garantem a restauração de sistemas e dados após um incidente, assegurando a continuidade do negócio.

X - Correlação e Gap *Analysis*

- A plataforma deverá identificar a posição atual de cada tecnologia e ferramenta de segurança em relação aos frameworks de referência NIST CSF v2 & AI RMF (*Artificial Intelligence Risk Management Framework*), NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS *Controls* v8 *Center for Internet Security*, ISO 27001 - *Information Security*, *Cybersecurity and Privacy protection*, *Cyber Insurance*, ISO 27701 - *Privacy Information Management*, ISO 27005 - *Information Security Risk Management*, ISO 22301 - *Business continuity management systems*, ISO 23894 - *Artificial intelligence — Guidance on risk management*. Essa correlação permitirá a realização de uma Análise de Lacunas (*Gap Analysis*) para determinar quais fases do ciclo de segurança não estão adequadamente cobertas por tecnologias existentes ou quais soluções não estão sendo utilizadas em seu potencial máximo.

XI - Apontamento de Melhores Práticas

- Com base na análise das tecnologias existentes e na correlação com os frameworks de segurança, a plataforma deverá, por meio de sua inteligência artificial, apontar e sugerir as melhores práticas para o aprimoramento da segurança. Isso inclui:

  - Recomendações de Otimização: Sugestões para o uso mais eficaz de tecnologias já implementadas.

  - Sugestões de Novas Ferramentas: Recomendações de tecnologias e ferramentas que podem cobrir lacunas identificadas nas fases do ciclo de segurança.

  - Plano de Ação: Geração de um plano de ação estruturado para a implementação das melhorias propostas.

- A solução deverá demonstrar a capacidade de correlacionar cada sugestão a um ou mais controles específicos dos frameworks NIST, CIS *Controls* ou ISO 27001, fornecendo um roteiro claro e auditável para a melhoria contínua da postura de segurança da CONTRATANTE.

XII - Integração e Avaliação de Maturidade e Conformidade

- A plataforma deverá ser intrinsecamente capaz de se integrar com sistemas de SIEM (*Security Information and Event Management*), proporcionando um processo de monitoramento e auditoria de segurança automatizado. Essa integração é fundamental para a transição de um modelo de gestão reativo para um modelo proativo.

- Integração com SIEM: A plataforma deverá consumir os dados e eventos de segurança gerados pelo SIEM, correlacionando-os com os riscos e controles mapeados no ambiente. Essa integração permitirá que a pontuação de risco seja atualizada em tempo real com base em eventos de segurança detectados. Utilização de inventário por meio de agente com consolidação do *Benchmark CIS* para *Hardering*.

XIII - Avaliação de Níveis de Maturidade

- A plataforma deverá fornecer uma avaliação clara e mensurável do nível de maturidade cibernética e corporativa da CONTRATANTE.

- Realizar a mensuração do nível de maturidade em conformidade com o referencial adotado, adotando-se métrica escalar de 1 a 5, onde o índice 1 representa o estágio inicial e o índice 5 representa o estágio de otimização dos processos , como sugerido pelo modelo CMMI (*Capability Maturity Model Integration*) , resultando uma classificação da maturidade da segurança da informação em cinco níveis distintos:

    o Nível 1 - Inicial: Processos imprevisíveis e reativos.
    o Nível 2 - Gerenciado: Processos definidos e gerenciados de forma básica.
    o Nível 3 - Definido: Processos padronizados e documentados.
    o Nível 4 - Quantitativamente Gerenciado: Processos medidos e controlados quantitativamente.
    o Nível 5 - Otimizado: Melhoria contínua e inovação dos processos.

- Pontuação de Risco (0 a 10): A plataforma deverá apresentar uma pontuação consolidada de risco, variando de 0 (risco baixo) a 10 (risco alto), para fornecer uma visão executiva e técnica do panorama de segurança.

XIV - Indicação de Percentuais de Atingimento de Frameworks

- A plataforma deverá indicar, de forma visual e quantitativa, os percentuais de atingimento de conformidade com os seguintes frameworks e regulamentações:

    - NIST CSFv2
    - NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*)
    - NIST SP 800-12 - Introdução à Segurança da Informação
    - NIST SP 800-39 - Gestão de Riscos Organizacionais
    - NIST SP 800-88 - Sanitização de Mídias
    - AI RMF (*Artificial Intelligence Risk Management Framework*)
    - CIS *Controls* v8
    - ISO 27000 (incluindo a ISO 27001)
    - ISO 27701 - *Privacy Information Management*
    - ISO 27005 - *Information Security Risk Management*

- ISO 22301 - *Business continuity management systems*
- ISO 23894 - *Artificial intelligence — Guidance on risk management* .
- PCI/DSS
- HIPAA
- LGPD
- GDPR
- Seguro Cibernético
- Auditorias (personalizáveis)

- Essa funcionalidade permitirá à CONTRATANTE identificar rapidamente as áreas de não conformidade, priorizar a implementação de controles e demonstrar o progresso em relação aos padrões de mercado, o que é fundamental para auditorias e para a gestão da governança.
- A plataforma deverá fornecer relatórios e painéis (dashboards) que correlacionem a pontuação de risco, o nível de maturidade e os percentuais de conformidade, garantindo uma visão unificada e completa da postura de segurança.
- A plataforma devera avaliar o uso de tecnologias e ferramentas de segurança da informação no ciclo de governança, identidade, proteção, detecção de ameaças, resposta a incidentes e recuperação.

XV - Controles para Ferramentas e Processos

- A plataforma deverá ser capaz de gerenciar, monitorar e auditar, de forma abrangente, os controles de segurança, correlacionando-os com as tecnologias e processos da CONTRATANTE.

XVI - Governança e Gestão de Riscos

- Estratégia de Gerenciamento de Risco: Suporte para a definição, implementação e monitoramento de uma estratégia de gerenciamento de risco.
- Funções, Responsabilidades e Autoridades: Mapeamento e acompanhamento de funções, responsabilidades e autoridades relacionadas à segurança da informação.
- Políticas de Segurança da Informação e Regras: Gerenciamento centralizado de políticas, incluindo a criação, revisão, aprovação e rastreamento da sua implementação.
- Supervisão e Auditoria: Funcionalidades que facilitem a supervisão e a realização de auditorias internas e externas, com a coleta de evidências e o rastreamento de não conformidades.
- Gerenciamento de Risco da Cadeia de Suprimentos de Segurança Cibernética: Avaliação e monitoramento de riscos associados a fornecedores e parceiros.

- Melhoria Continuada: Ferramentas para a gestão do ciclo de melhoria contínua, com a medição do progresso e o apontamento de planos de ação.

XVII - Proteção e Defesa, integrado com SIEM

- Gerenciamento de Ativos: Visibilidade e controle sobre o inventário de ativos (hardware, software e informações), correlacionando-os com os respectivos proprietários e classificações de criticidade.
- Gerenciamento de Identidade, Autenticação e Controle de Acesso: Controles que validem a implementação de soluções de IAM, PAM e NAC.
- Conscientização e Treinamento: Acompanhamento da aplicação de políticas de conscientização e treinamento em segurança para a equipe.
- Segurança de Dados: Controles que avaliam a implementação de medidas de proteção de dados, como criptografia, prevenção de perda de dados (DLP) e políticas de retenção.
- Segurança de Plataforma: Avaliação da segurança de sistemas operacionais, aplicações e serviços em nuvem.
- Resiliência de Infraestrutura de Tecnologia: Monitoramento e análise da resiliência da infraestrutura de TI contra falhas e eventos adversos.

XVIII - Detecção, Resposta e Recuperação de Incidentes: SIEM

- Monitoramento Contínuo: Capacidade de monitorar continuamente o ambiente para detectar atividades anômalas e indicadores de comprometimento.
- Análise de Eventos Adversos: Análise e correlação de eventos de segurança provenientes de diversas fontes, para identificar incidentes potenciais.
- Gerenciamento de Incidentes: Funcionalidades para o gerenciamento do ciclo de vida de um incidente, incluindo o registro, a classificação, a priorização e o rastreamento.
- Análise de Incidentes: Ferramentas que suportem a análise detalhada de incidentes para determinar a causa raiz, o vetor de ataque e o impacto.
- Relatórios e Comunicação de Resposta a Incidentes: Geração de relatórios de incidentes e comunicação das ações tomadas às partes interessadas.
- Mitigação e Recuperação:

  o Mitigação de Incidentes: Apontamento de planos de ação para a mitigação dos incidentes.
  o Recuperação de Incidentes: Avaliação da execução do plano de recuperação para restabelecer os serviços e sistemas afetados.
  o Comunicação de Recuperação de Incidentes: Apoio à comunicação durante o processo de recuperação, garantindo que as partes interessadas sejam informadas do status.

- A plataforma deverá ser capaz de gerar relatórios e dashboards que demonstrem a implementação e a eficácia de cada um dos controles acima,

fornecendo um roteiro claro e auditável para a gestão da segurança da informação.

XIX - Avaliação de Processos, Recursos e Controles

- A plataforma deverá ser capaz de avaliar, de forma integrada, o uso de processos, recursos tecnológicos, humanos e a implementação de controles de segurança, conforme as seguintes categorias:

  a) Identificação e Proteção

  - Inventário e Controle de Ativos de Software: A plataforma deverá ter a funcionalidade de criar e manter um inventário completo e atualizado de todos os softwares licenciados e instalados nos ativos de TI.
  - Proteção de Dados: A plataforma deverá avaliar a implementação de medidas de segurança de dados, como a criptografia de dados em repouso e em trânsito, a classificação de dados, e a prevenção de perda de dados (DLP).
  - Configuração Segura de Ativos Corporativos e Software: Avaliação da conformidade das configurações de segurança de sistemas operacionais, aplicações e dispositivos, comparando-as com benchmarks de segurança reconhecidos (e.g., CIS Benchmarks).
  - Gerenciamento de Contas e Controle de Acesso: A plataforma deverá avaliar a eficácia das políticas de gerenciamento de contas, incluindo a criação, modificação e exclusão de contas, e o controle de acesso a sistemas e dados (IAM, NAC).
  - Gerenciamento Contínuo de Vulnerabilidades: A solução deverá ser capaz de gerenciar os resultados de scans de vulnerabilidade, priorizar as correções com base no risco e rastrear o progresso da remediação.
  - Gerenciamento de Log de Auditoria: A plataforma deverá avaliar a coleta, o armazenamento e a análise de logs de segurança, garantindo que as atividades críticas e suspeitas estejam sendo devidamente registradas para fins de auditoria e investigação

  b) Detecção e Resposta

  - Proteções de E-mail e Navegador da Web: A plataforma deverá avaliar a implementação de controles de segurança para e-mails e navegadores, como filtragem de conteúdo, proteção contra *phishing* e *malware*, e segurança de endpoints.
  - Defesas Contra Malware: Avaliação da eficácia das soluções de proteção contra malware, como antivírus e *endpoint detection and response* (EDR).
  - Recuperação de Dados: A plataforma deverá avaliar a existência e a eficácia das políticas e dos processos de recuperação de dados, como o backup regular e a restauração de dados críticos.
  - Gerenciamento de Infraestrutura de Rede: Avaliação da segurança da

infraestrutura de rede, incluindo a segmentação de rede, a configuração de firewalls e o controle de acesso.

- Monitoramento e Defesa de Rede: Avaliação da capacidade de monitoramento do tráfego de rede para detectar ameaças e atividades anômalas (NDR).
- Conscientização sobre Segurança e Treinamento de Habilidades: A plataforma deverá ser capaz de rastrear a participação da equipe em treinamentos de segurança e avaliar o nível de conscientização geral da organização.
- Gerenciamento de Provedores de Serviços: Avaliação dos riscos de segurança associados a provedores de serviços de terceiros.

c) Segurança e Gerenciamento de Aplicações

- Segurança de Software de Aplicação: A plataforma deverá avaliar a implementação de medidas de segurança no ciclo de vida de desenvolvimento de software (SDLC), incluindo testes estáticos e dinâmicos (SAST / DAST).
- Gerenciamento de Resposta a Incidentes: A plataforma deverá avaliar a eficácia do plano de resposta a incidentes, incluindo a orquestração e automação de tarefas.
- Teste de Penetração: A plataforma deverá facilitar o gerenciamento e a análise dos resultados de testes de penetração realizados na infraestrutura e em aplicações, correlacionando as descobertas com a pontuação de risco.
- A plataforma deve fornecer painéis e relatórios que consolidem todas as informações acima, oferecendo uma visão integrada e quantitativa sobre a maturidade da segurança da CONTRATANTE.

XX - Funções da Plataforma

- A plataforma deverá ter, obrigatoriamente, as seguintes funções para fornecer uma visão completa e multifacetada da postura de segurança da instituição:

  a) Visão Corporativa

  - A plataforma deve oferecer painéis e relatórios executivos que traduzam os riscos técnicos e operacionais em termos de impacto para o negócio. Esta visão se concentrará em:
    - Impactos Financeiros: Estimativa de perdas financeiras potenciais (custos de remediação, multas, interrupção de negócios).
    - Impactos Legais: Avaliação da conformidade com regulamentações (LGPD, GDPR, HIPAA, etc.) e o risco de ações judiciais.
    - Impactos de Reputação: Análise do risco de dano à marca e à reputação da instituição decorrente de incidentes de segurança.

b) Visão Técnica

- A plataforma deve proporcionar aos profissionais de segurança uma análise aprofundada e em tempo real do ambiente técnico. Esta visão incluirá:
    - Vulnerabilidades: Detalhamento de vulnerabilidades em sistemas, aplicativos e infraestrutura.
    - Falhas em Sistemas: Identificação de *misconfigurations* e desvios de padrões de segurança.
    - Ameaças em Tempo Real: Monitoramento contínuo de indicadores de comprometimento (IOCs) e atividades maliciosas.

c) Visão de Governança

- Esta funcionalidade deve apresentar o nível de maturidade e conformidade da instituição em relação às suas políticas e aos frameworks de segurança. A plataforma deverá demonstrar:
    - Nível de Atingimento Percentual: Indicadores percentuais de conformidade com as políticas internas e frameworks como NIST, CIS, ISO 27001, com base nas regras de governança, identidade, proteção, detecção de ameaças, resposta a incidentes e recuperação.
    - Rastreabilidade de Controles: A capacidade de rastrear a implementação de cada controle de segurança em relação aos objetivos de governança.

d) Pontuação de Conformidade

- A plataforma deverá fornecer uma pontuação consolidada por conformidade, com base na análise de três pilares:
    - Uso de Tecnologias: Avaliação da efetividade das tecnologias de segurança implementadas.
    - Aplicação do Processo de Controle: Mensuração da aderência aos procedimentos operacionais e às políticas.
    - Controles Manuais, Automatizados e Auditados: Diferenciação e pontuação para controles que são executados de forma manual, automatizada ou que passaram por processos de auditoria.

e) Medição de Controles

- A solução deverá fornecer uma medição percentual dos controles, mostrando o progresso da implementação e a eficácia de cada um. Além disso, a plataforma deve ir além da simples medição, oferecendo:
    - Apontamento de Planos de Ação: Geração de um roteiro detalhado para a implementação ou aprimoramento dos controles.

- Sugestões para Melhorias: Recomendações de tecnologias, processos e serviços que podem otimizar o desempenho dos controles e fechar lacunas de segurança.

f) Níveis de Maturidade e Frameworks

- A solução deve apresentar os níveis de maturidade utilizando o modelo de classificação do padrão CMMI, classificando a maturidade da segurança em cinco níveis: Inicial, Gerenciado, Definido, Quantitativamente Gerenciado e Otimizado. Esses níveis de maturidade deverão ser correlacionados com os frameworks, NIST CSFv2, CIS Controls v8 e ISO 27000.

- A plataforma deverá destacar os controles atrelados a domínios, controles e políticas dos seguintes frameworks: NIST, CIS, HIPPA, PCI-DSS, LGPD, FIM e GDPR.

- Adicionalmente, deve permitir o controle de auditoria de conformidade de políticas e controles de forma manual e automatizada.

g) Integração e Compatibilidade

- A solução deverá ser compatível com diversas ferramentas de segurança e permitir a integração com sistemas como:

  - SIEM (*Security Information Event Management*) nativo da solução ou ferramentas homologadas via API.

  - Monitoramento *Deep Dark Web*.

  - GRC.

  - Soluções de Privacidade de Dados (nativas ou homologadas via API).

  - NDR.

  - Gerenciamento de Patches e Vulnerabilidades

XXI - Avaliação de Ferramentas de Segurança da Informação

- A plataforma deverá ser capaz de avaliar e correlacionar a implementação e a eficácia das seguintes categorias de ferramentas e tecnologias de segurança da informação, conforme o ciclo de vida da segurança cibernética e os domínios de proteção. A solução deve atuar como um painel de controle único para auditar a presença e a configuração dessas ferramentas, fornecendo uma visão consolidada da postura de segurança da CONTRATANTE.

  - Governança e Conformidade

    - PRIVACY & GRC: Avaliação de ferramentas que apoiam a gestão de privacidade (LGPD/GDPR) e a governança, risco e conformidade (GRC).

    - GOVERNANCE / RISK: Análise de soluções dedicadas à governança e gestão de risco cibernético.

        - THIRD PARTY RISK MGMT: Avaliação de ferramentas para gerenciar os riscos de segurança associados a terceiros e à cadeia de suprimentos.
        - MATURITY MONITORING: Monitoramento de soluções que medem a maturidade da segurança da informação.
        - SOFTWARE SUPPLY CHAIN: Análise da segurança na cadeia de suprimentos de software.
    - Proteção e Defesa
        - DATA SECURITY: Avaliação de tecnologias para proteção de dados em geral.
        - DLP CLOUD & AGENT: Análise de soluções de Prevenção de Perda de Dados em ambientes de nuvem e on-premise via agentes.
        - ENCRIPTY ENDPOINT/SERVER/DATABASE/DATA NETWORK: Avaliação de tecnologias de criptografia para endpoints, servidores, bancos de dados e dados em trânsito.
        - PATCH MANAGEMENT & VULNERABILITY MANAGEMENT: Análise de ferramentas de gerenciamento de patches e vulnerabilidades, incluindo IAST (Interactive Application Security Testing) e funcionalidades de descoberta.
        - ASSET MANAGEMENT (MANUAL & AUTOMATIC): Avaliação de sistemas de gerenciamento de ativos, tanto manuais quanto automatizados.
        - PHISHING TEST/AWARENESS PLATFORM: Análise de plataformas de testes de phishing e conscientização em segurança.
        - API/WAF & NFW WAF: Avaliação de soluções de Web Application Firewall (WAF) e segurança de APIs.
        - NFW - IPS/IDS: Análise de sistemas de prevenção e detecção de intrusão (IPS/IDS) em firewalls de próxima geração.
        - ANTI DDOS & DDoS PROTECTION AND RESPONSE: Avaliação de soluções de proteção contra-ataques de negação de serviço distribuída (DDoS).
        - DNS SECURITY: Análise de tecnologias para segurança de DNS.
        - BACKUP - ON PREMISE/CLOUD & DISASTER RECOVERY: Avaliação de soluções de backup e recuperação de desastres, tanto em ambientes locais quanto em nuvem.
        - DATA SAFE AND DISPOSE TOOLS: Análise de ferramentas para proteção e descarte seguro de dados.
        - DIGITAL CERTIFICATE: Avaliação do gerenciamento e uso de

certificados digitais.

- MDM-SOFTWARE MANAGEMENT: Análise de soluções de gerenciamento de dispositivos móveis.
- GPO: Avaliação da configuração e gestão de políticas de grupo.
- CASB & SASE: Análise de soluções de segurança de acesso à nuvem e Secure Access Service Edge.
- ZTNA & ZTNS: Avaliação de arquiteturas de segurança Zero Trust para acesso à rede e serviços.
- ZT/VLAN/SEG: Análise de segmentação de rede.

- Detecção e Resposta
  - NDR & XDR & EDR: Avaliação de soluções de detecção e resposta para rede, estendida e endpoint.
  - ANTI VIRUS: Análise de softwares antivírus.
  - THREAD INTEL: Avaliação de plataformas de inteligência de ameaças.
  - BASTION-HOST & SANDBOX: Análise de Bastion hosts e ambientes de sandbox para análise de malware.
  - HONEYPOT: Avaliação do uso de honeypots para detecção de ameaças.
  - EDR/XDR INCIDENT RESPONSE: Análise de plataformas de orquestração, automação e resposta a incidentes.
  - TESTES DE SEGURANÇA (SAST, DAST, APPSEC/AST/APISEC): Avaliação de ferramentas para testes de segurança em código, aplicações e APIs.
- Identidade e Acesso
  - PAM & IAM: Avaliação de soluções de gerenciamento de acesso privilegiado e de identidade e acesso.
  - NAC: Análise de sistemas de controle de acesso à rede.
  - SAFE PASSWORD & IDENTITY & FEDERATION: Avaliação de soluções de gerenciamento seguro de senhas e federação de identidades.
- Monitoramento e Análise
  - SIEM: Avaliação da solução de gerenciamento de informações e eventos de segurança.
  - ITSM - SEC: Análise de sistemas de gerenciamento de serviços de TI.
  - OBSERVABILITY (IT, PHYSICAL, PATRIMONIAL): Avaliação

de ferramentas de observabilidade e monitoramento de ativos físicos e de TI.

- TOPOLOGY-DOCUMENTATION-ARQUITECH: Análise de ferramentas para documentação de topologia e arquitetura.
- CLOUD SECURITY: Avaliação de soluções de segurança para ambientes em nuvem.
- VM SEC: Análise da segurança de máquinas virtuais.
- IOT/OT SECURITY: Avaliação de soluções de segurança para ambientes de Internet das Coisas e Tecnologia de Operação.
- AI SECURITY: Análise de ferramentas de segurança baseadas em inteligência artificial.
- NETFLOW: Avaliação do monitoramento de tráfego de rede.
- VPN: Avaliação do uso de redes privadas virtuais.
- CLOUD SEC VUL / CONTEINER SEC / IA SEC MICROSERVICES: Análise da segurança de vulnerabilidades em nuvem, contêineres e microsserviços.

XXII - Avaliação de Riscos e Conformidade com Políticas

- A plataforma deverá fornecer uma avaliação clara e mensurável dos riscos e do nível de conformidade com as políticas internas da organização.
    - Pontuação de Risco: A solução deverá apresentar uma pontuação de risco intuitiva, variando de 0 (risco mínimo) a 10 (risco crítico). Essa pontuação deve ser alimentada por um contexto de políticas de segurança da informação, que correlaciona as vulnerabilidades, as ameaças e as não conformidades com o impacto potencial para o negócio.
    - Percentuais de Atingimento: A plataforma deverá gerar relatórios detalhados que indiquem a porcentagem de conformidade atingida para cada um dos seguintes frameworks e regulamentações reconhecidas: NIST CSF v2 & AI RMF (Artificial Intelligence Risk Management Framework), NIST SP 800-30 - Avaliação de Risco (Risk Assessments), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS Controls v8 Center for Internet Security, ISO 27001 - Information Security, Cybersecurity and Privacy protection, Cyber Insurance, ISO 27701 - Privacy Information Management, ISO 27005 - Information Security Risk Management, ISO 22301 - Business continuity management systems, ISO 23894 - Artificial intelligence — Guidance on risk management. Esses relatórios devem permitir a priorização de esforços onde há lacunas mais críticas.

XXIII - Controles e Políticas

- A plataforma deverá destacar os controles de segurança e correlacioná-los,

de forma obrigatória, com as seguintes políticas e planos:

- Política de Segurança da Informação
- Plano Estratégico de Segurança da Informação
- Risk Management Framework
- Política de Fornecedores e Cadeia de Suprimentos
- Política de Privacidade de Dados
- Política de Governança de Tecnologia e Anticorrupção
- Política de Segurança - Recursos Humanos
- Política de Melhoria Continuada e Auditoria Interna e Externa
- Política de Gerenciamento de Ativos
- Política de Gerenciamento de Vulnerabilidades
- Política de Gerenciamento de Inteligência de Ameaças
- Processo de Gerenciamento Mudanças
- Plano de Continuidade de Negócios
- Plano de Resposta a Incidentes Cibernéticos
- Plano de Resposta a Incidentes de Privacidade de Dados
- Política de Uso da Internet
- Política de Segurança Física
- Política de Gerenciamento de Acesso
- Política de Gerenciamento de Conscientização
- Política de Criptografia
- Política de Cópias de Segurança
- Política de Desenvolvimento Seguro
- Política de Gerenciamento e Proteção de Endpoint
- Política de Teletrabalho e BYO
- Política de Gerenciamento de Software, Dados, Imagens, Padrões e Hardering
- Política de Infraestrutura e Cloud Segura
- Política de Inteligência Artificial
- Política de Monitoramento de Segurança

- Política de Incidente de Segurança da Informação
- Política de Teste e Simulações de Ataques (Pen-test)
- Política de Problemas/Recuperação de Segurança da Informação
- A plataforma deve fornecer um mecanismo para que a CONTRATANTE possa comprovar a implementação de cada política e seus respectivos controles, garantindo que o progresso possa ser auditado e demonstrado com evidências claras.

XXIV - Relatórios e Instrumentos de Auditoria

- A plataforma deve ser capaz de gerar relatórios detalhados que sirvam como um instrumento de auditoria robusto, avaliando a aderência da CONTRATANTE a políticas internas e frameworks de segurança reconhecidos.
    - Avaliação por Políticas e Níveis de Maturidade: Os relatórios deverão avaliar a conformidade de cada política e seus controles, correlacionando-os com os Níveis de Maturidade do padrão de classificação CMMI e com os frameworks NIST, CIS, ISO 27.000 e Seguro Cibernético. Essa correlação permitirá uma análise cruzada, mostrando como a maturidade de um processo impacta na conformidade com os padrões de mercado.
    - Controles Mínimos por Política: Os relatórios deverão destacar, de forma clara, o nível de implementação e conformidade para o número mínimo de controles exigidos para cada política, conforme a seguinte tabela:

Política / Plano	Controles Mínimos Requeridos
Política de Segurança da Informação	17
Plano Estratégico de Segurança da Informação	7
Risk Management Framework	10
Política de Fornecedores e Cadeia de Suprimentos	26
Política de Privacidade de Dados	10
Política de Governança de Tecnologia e Anticorrupção	7
Política de Melhoria Contínua e Auditoria Interna e Externa	16
Política de Gerenciamento de Ativos	31
Política de Gerenciamento de Vulnerabilidades	22
Política de Gerenciamento de Inteligência de Ameaças	11
Processo de Gerenciamento Mudanças	7
Plano de Continuidade de Negócios	7
Plano de Resposta a Incidentes Cibernéticos	7
Plano de Resposta a Incidentes de Privacidade de Dados	7
Política de Uso da Internet	8
Política de Segurança Física	7
Política de Gerenciamento de Acesso	41
Política de Gerenciamento de Conscientização	13

Política de Criptografia	13
Política de Cópias de Segurança	12
Política de Desenvolvimento Seguro	22
Política de Gerenciamento e Proteção de *Endpoint*	23
Política de Teletrabalho e BYO	10
Política de Gerenciamento de Software, Imagens, Padrões e *Hardening*	22
Política de Infraestrutura e Cloud Segura	35
Política de Monitoramento de Segurança	48
Política de Incidente de Segurança da Informação	32
Política de Teste e Simulações de Ataques (*Pen-test*)	11
Política de Problemas de Segurança da Informação	5

- Controle de Recomendações e Lacunas: Para cada lacuna de conformidade ou item não atendido, o relatório deverá, obrigatoriamente, fornecer recomendações detalhadas e um plano de ação sugerido. Essa funcionalidade transforma o relatório em uma ferramenta prática para a melhoria contínua da segurança.

- Consolidação para Auditoria: O relatório final deverá consolidar o atingimento de conformidade de forma que possa ser facilmente utilizado como evidência em processos de auditoria interna e externa, demonstrando o progresso da organização em relação a seus objetivos de segurança e conformidade.

5.15. SERVIÇO DE SETUP E IMPLANTAÇÃO

5.15.1. Considerando a complexidade intrínseca aos processos de gestão de riscos, conformidade normativa e maturidade em segurança da informação, torna-se indispensável a alocação de profissionais qualificados, com a finalidade de assegurar a execução do setup, a implantação, a parametrização, a análise crítica, a validação e a aplicação de políticas de segurança da informação na plataforma objeto da presente contratação.

5.15.2. A disponibilização deste serviço especializado visa garantir a plena e correta utilização da solução tecnológica, abrangendo a configuração, o tratamento e a interpretação dos dados nela inseridos, de modo a viabilizar a implementação eficiente de controles manuais e automatizados. Dessa forma, busca-se promover a mitigação de riscos, o alinhamento às melhores práticas nacionais e internacionais, bem como a elevação contínua do nível de segurança organizacional, em estrita observância ao que dispõe a tabela de descrição dos itens de licenciamento.

5.15.3. Os serviços serão utilizados para as seguintes atividades:

5.15.4. Setup e Implantação da Plataforma

5.15.4.1. O fornecedor deverá conduzir o processo de implantação da plataforma, incluindo o setup e a customização, para que a solução esteja operacional e alinhada aos objetivos e requisitos técnicos e de negócio da PRODESP.

5.15.4.2. Fases do Processo de Implantação:

- Planejamento e Kick-off:
    - Reunião de alinhamento inicial com as equipes da PRODESP e CONTRATADA para

definição de cronograma, papéis e responsabilidades.

- Detalhar os objetivos e escopo da implantação da plataforma.

- Instalação e Configuração:
  - A plataforma será fornecida na modalidade SaaS (*Software as a Service*) e ficará hospedada no ambiente da CONTRATADA.
  - Configuração do ambiente em SaaS no Brasil com redundância de zonas de disponibilidade (*Availability Zones*) para alta resiliência e failover automático.
  - Configuração da arquitetura em conformidade com a documentação da plataforma
  - Implementação de medidas de segurança na infraestrutura, como isolamento de rede (VNet), controle de tráfego (NSG) e criptografia AES-256 no armazenamento.

5.15.4.3. Conclusão dos Serviços de Setup e Implantação:

- Após a conclusão dos serviços de setup e implantação, a plataforma deverá estar completamente disponível e funcional, atendendo integralmente a todas as definições técnicas, funcionais e de segurança especificadas neste Termo de Referência. A homologação da plataforma, por parte da CONTRATANTE, será realizada com base na comprovação de que a solução está em pleno funcionamento, com todas as integrações configuradas, os módulos operacionais e os relatórios de risco, maturidade e conformidade sendo gerados de forma precisa e automatizada, conforme as condições estabelecidas.

5.15.4.4. Serviço Mensal:

- Este serviço mensal deverá atender os itens abaixo:
  - Análise e Validação de Políticas de Segurança
  - Avaliar as políticas existentes de governança, identidade, proteção, detecção, resposta e recuperação.
  - Validar a aderência dessas políticas aos *frameworks* como NIST CSF v2 & AI RMF (*Artificial Intelligence Risk Management Framework*), NIST SP 800-30 - Avaliação de Risco (*Risk Assessments*), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS *Controls* v8 *Center for Internet Security*, ISO 27001 - *Information Security, Cybersecurity and Privacy protection, Cyber Insurance*, ISO 27701 - *Privacy Information Management*, ISO 27005 - *Information Security Risk Management*, ISO 22301 - *Business continuity management systems*, ISO 23894 - Artificial intelligence — *Guidance on risk management*, entre outros.
  - Sugerir atualizações ou ajustes com base em melhores práticas e requisitos regulatórios.

5.15.4.5. Relatórios de Maturidade:

- Geração de Relatório Consolidado de Maturidade Cibernética, que fornecerá a visão unificada da postura de segurança do órgão com base em três frameworks de referência: NIST, CIS Controls, ISO 27001 e LGPD.

- Relatório de Maturidade NIST *Cybersecurity Framework* (CSF):

- Apresentação do Nível de Maturidade Atual do órgão (e.g., Nível 2 - Risco Repetível para Nível 3 - Risco Adaptativo). O relatório deve detalhar o Atingimento Percentual em cada uma das cinco funções do NIST: Identificar, Proteger, Detectar, Responder e Recuperar, destacando os gaps estratégicos e o progresso do *roadmap* de melhoria.

- Relatório de Aderência aos CIS *Controls* (Centro de Segurança da Internet):

- Demonstração do score de aderência e da eficácia dos controles de segurança mais críticos. O relatório deve priorizar a remediação com base na capacidade dos controles de deter as táticas de ataque mais comuns. Ideal para o público técnico, mostrando a eficiência na implementação da segurança básica.

- Relatório de Conformidade ISO/IEC 27001 (Sistema de Gestão da Segurança da Informação – SGSI):

- Avaliação formal da aderência aos requisitos da norma (Seção 4 a 10) e aos controles do anexo A (ISO 27002). O Consultor deve atestar a existência e a eficácia dos controles de Pessoas e Processos (e.g., Gestão de Acessos, Treinamento, Política de Continuidade), crucial para a demonstração de conformidade em auditorias externas.

- Relatório de Status de Conformidade LGPD

- Traduzir os resultados complexos de segurança (NIST, CIS, ISO) em termos de negócio claros para o Comitê de Governança, facilitando a tomada de decisão sobre o aporte de capital e recursos humanos.

5.15.4.6. Geração e Validação de Controles de Auditoria

- Criar e revisar controles manuais e automatizados com base nos domínios e políticas da organização.

- Garantir que os controles estejam alinhados com os requisitos de auditorias como PCI, ISO 27001, SOC2

5.15.4.7. Pontuação de Conformidade e Planos de Ação

- Avaliar o nível de conformidade por tecnologia, processo e controle.

- Medir o percentual de aplicação dos controles e sugerir:

- Tecnologias adequadas

- Processos otimizados

- Serviços complementares

5.15.4.8. Automação e Monitoramento Contínuo

- Configurar e manter os controles automatizados de conformidade.

- Garantir que os dados estejam sempre atualizados para geração de relatórios em tempo real.

5.15.4.9. O serviço deverá ser executado através de atividades a serem desenvolvidas em reuniões, presenciais e/ou virtuais, devendo-se focar no detalhamento do plano de execução dos serviços, contemplando a metodologia de gestão, macro programa, plano de comunicação, relatórios de status e interfaces.

5.15.4.10. Nas reuniões de início deverão obrigatoriamente ser tratados os temas:

- Aplicação da plataforma em seus aspectos direcionados à Administração Pública;
- A importância da conformidade para a PRODESP;
- O projeto de adequação ao ambiente da CONTRATADA;
- A definição e apresentação dos relatórios mensais.

5.15.4.11. A CONTRATADA deverá entregar, para validação da PRODESP, pelo menos, 02 (dois) RELATÓRIOS com conteúdo definidos a seguir:

a) Relatório de projeto de implantação (“AS BUILT”):

- Contempla-se neste Relatório, a etapa de planejamento para a implantação do objeto especificado neste anexo;
- O relatório deverá contemplar e detalhar todas as etapas da instalação, isto é, os serviços de planejamento, instalação, integração e pré-operação;
- O relatório deverá contemplar cronograma informando o prazo para a execução de cada etapa do serviço contemplado neste relatório;
- O relatório deverá contemplar a arquitetura desenhada pela CONTRATADA;
- O prazo máximo para a entrega do Relatório de projeto de implantação pela CONTRATADA à PRODESP é de 15 dias a contar da data da 1ª reunião de acompanhamento da execução do contrato.

b) Relatório final de implantação

- Neste documento deverão constar todas as informações geradas pela CONTRATADA abordando os aspectos da arquitetura implantada, configuração, testes e integração ao ambiente da PRODESP;
- O Relatório final de implantação deverá ser fornecido no prazo máximo de 15 (quinze) dias a contar da data de conclusão e validação do SERVIÇO DE IMPLANTAÇÃO especificado.

5.15.4.12. Todos os relatórios de projeto “As Built” serão considerados como efetivamente entregues e aceitos somente após a validação pela equipe técnica da PRODESP que se fará no prazo máximo de 10 (dez) dias a contar da respectiva entrega;

5.15.4.13. Os relatórios deverão ser apresentados em via impressa e/ou meio digital, conforme acordado entre as partes;

5.15.4.14. O software empregado na confecção dos textos integrantes das documentações deverá ser totalmente compatível com o MS Word em versão mais recente;

5.15.4.15. Os relatórios deverão ser emitidos em papel timbrado da CONTRATADA e deverão conter o nome, data e assinatura do Gestor de Projeto da CONTRATADA.

5.16. LICENCIAMENTO DOS DEVICES

5.16.1. A Plataforma deverá realizar com base na quantidade de devices (endpoints) ativos, integrados e efetivamente monitorados no ambiente corporativo da CONTRATANTE. Para fins deste instrumento, consideram-se endpoints todos os dispositivos conectados à infraestrutura tecnológica da organização, incluindo, mas não se limitando a, servidores físicos

e virtuais, estações de trabalho, notebooks, dispositivos móveis, equipamentos de rede, appliances de segurança, ativos em nuvem e quaisquer outros dispositivos ou ativos tecnológicos passíveis de monitoramento pela solução.

5.16.2. Para fins de dimensionamento contratual e precificação, fica estabelecido como referência o limite de até 10.000 (dez mil) *endpoints* monitorados por mês.

5.16.3. O modelo de licenciamento por *endpoint* adotado pela CONTRATADA possui como finalidade assegurar proporcionalidade, previsibilidade financeira, escalabilidade operacional e aderência entre o volume de ativos monitorados e os serviços efetivamente prestados. Tal modelo permite que a PRODESP mantenha controle objetivo sobre a utilização das licenças, garantindo maior eficiência na gestão dos ativos tecnológicos, na governança de TI, na segurança cibernética e no acompanhamento contínuo da superfície de exposição digital da organização.

5.16.4. A contabilização dos endpoints considerará exclusivamente os dispositivos efetivamente integrados, comunicantes e monitorados pela Plataforma durante o período mensal de referência, desconsiderando ativos descontinuados, inativos, descomissionados ou não operacionalizados no ambiente monitorado.

5.17. ASSESSMENT

5.17.1. A Plataforma devera realizar assessment continuo de avaliações automatizadas de maturidade e postura de Segurança da Informação sobre os devices (endpoints) ativos, integrados e efetivamente monitorados no ambiente corporativo da CONTRATANTE.

5.17.2. Para fins deste instrumento, consideram-se devices (endpoints) todos os dispositivos conectados à infraestrutura tecnológica da CONTRATANTE, incluindo, mas não se limitando a, servidores físicos e virtuais, estações de trabalho, notebooks, dispositivos móveis, equipamentos de rede, appliances de segurança, ativos em nuvem e demais ativos tecnológicos passíveis de monitoramento e avaliação pela plataforma.

5.17.3. A solução realizará ciclos automatizados de assessment em periodicidade contínua de até 1 (uma) hora, compreendendo verificações técnicas, análise de postura de segurança, identificação de vulnerabilidades, aderência a frameworks, maturidade de controles e consolidação de indicadores relacionados ao ambiente monitorado.

5.17.4. Para fins de dimensionamento contratual, acompanhamento operacional e faturamento, fica estabelecido o limite de até 730 (setecentos e trinta) assessments mensais, entendidos como ciclos formais, automatizados e consolidados de avaliação da postura de Segurança da Informação executados pela plataforma sobre o ambiente monitorado da CONTRATANTE.

5.17.5. O modelo de licenciamento por Assessment possui como finalidade assegurar proporcionalidade entre a capacidade de processamento analítico da plataforma, o volume de ativos monitorados e os serviços efetivamente disponibilizados, garantindo previsibilidade operacional, rastreabilidade das análises realizadas, escalabilidade da solução e aderência.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de execução:

6.1.1. A PRODESP, 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 (*kickoff*), com o objetivo de:

a) Alinhar a forma de comunicação entre as partes, que deverá ocorrer preferencialmente entre a PRODESP e a CONTRATADA;

b) Definir as providências necessárias para inserção da CONTRATADA no

ambiente de prestação dos serviços;

c) Definir as providências para a elaboração do Relatório de projeto de Implantação e a execução dos serviços;

d) Alinhar entendimento quanto aos modelos de execução e de gestão do contrato.

6.1.2. Mecanismos formais de comunicação:

6.1.2.1. São definidos como mecanismos formais de comunicação, entre a PRODESP e a CONTRATADA, os seguintes:

a) Ata de Reunião;

b) Ofício;

c) Canal de abertura de chamados;

d) E-mails.

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

6.2. TRANSFERÊNCIA DE CONHECIMENTO (*Hands On*)

6.2.1. A CONTRATADA deverá realizar transferência de conhecimento aos usuários e/ou agentes multiplicadores que farão uso da Plataforma.

6.2.2. As transferências de conhecimento poderão ser realizados de forma presencial e/ou remota, em datas e horários acordado entre as partes. Na ocasião da forma presencial, deverá ser ministrada nas dependências da PRODESP, cito à Rua Agueda Gonçalves, 240, Jardim Pedro Gonçalves - Taboão da Serra - SP.

6.2.3. A CONTRATADA deverá disponibilizar instrutores em número, competência e experiência profissional adequada ao transferência de conhecimento ser realizado.

6.2.4. A CONTRATADA será responsável pela especificação do conteúdo programático e da carga horária, de acordo com a atividade a ser desempenhada por cada tipo de usuário.

6.2.5. A transferência de conhecimento deverá dividida em 02 (duas) turma de até 10 alunos.

6.2.6. Carga Horária Total Sugerida: 80 horas

6.2.7. A CONTRATADA deverá apresentar em até 20 dias uteis após o início do projeto, um cronograma de treinamento abrangente e prático, abordando os seguintes tópicos principais:

a) Administração da Plataforma

b) Gestão de Riscos e Vulnerabilidades

c) Monitoramento de Maturidade e Conformidade

d) Governança de Segurança da Informação e Privacidade de Dados

e) Integração e Automação via API

f) Gerenciamento de Relatórios e Dashboards

6.2.8. Formato e Metodologia

6.2.8.1. A transferência de conhecimento deverá ser ministrada logo após a implantação da plataforma, em formato presencial e/ou remota. Será priorizado o aprendizado prático, com exercícios e estudos de caso para que os administradores possam aplicar os conhecimentos diretamente no ambiente da plataforma.

7. ESTIMATIVA DE DEMANDA

7.1. Conforme levantamento realizado pela equipe técnica da Gerência de Segurança da Informação utilizando como parâmetro a infraestrutura de segurança hoje disponibilizada no Data Center Prodesp, foi dimensionado as quantidades elencadas abaixo:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Plataforma de Governança e Maturidade em Cibersegurança	Un	01
2	Assessment	Un	8.760
3	Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede)	Un	10.000
4	Serviço de Setup/Implantação	Serviço Único	01
5	Serviço de Suporte/Manutenção e Serviço Mensal	Serviço Mensal	12
6	Serviço de Transferência de Conhecimento (*Hands On*) para turmas de até 10 alunos	Turma	02

8. PAPÉIS E RESPONSABILIDADES

8.1. São papéis desempenhados na gestão do contrato oriundo deste Termo de Referência:

Responsável/Função	Atribuições
Gestor do Contrato	Empregado PRODESP da área demandante, com capacidade funcional, técnica e operacional relacionada ao objeto da contratação, designado para ser o responsável por administrar e acompanhar o contrato, com o apoio da equipe de gestão, a fim de garantir a execução do objeto contratado, inclusive suas prorrogações e aditamentos, desde a sua assinatura até o seu encerramento. O encargo dessa responsabilidade, compreende também, observância da regularidade documental, na qualidade de preposto da PRODESP perante o Contratado, devendo informar a Administração sobre eventuais vícios, irregularidades ou baixa qualidade dos serviços prestados. Propor as sugestões para soluções que entender cabíveis para regularização das falhas, faltas e defeitos observados, bem como no que se refere à aplicação de sanções previstas no disposto nesta Norma.

Fiscal do contrato	Empregado PRODESP da área demandante, designado para auxiliar o Gestor do Contrato na fiscalização dos aspectos administrativos e técnicos da contratação.

8.2. Critérios de Aceitação:

8.2.1. A PRODESP emitirá o termo de aceite para a Plataforma, após a constatação de sua implantação/liberação, considerando as especificações técnicas contidas neste documento e observando os Níveis Mínimos de Serviço estabelecidos no item 8.3 - deste Termo de Referência.

8.2.2. A PRODESP emitirá o termo de aceite para o serviço de implantação/setup após a instalação da plataforma em ambiente de produção.

8.2.3. A PRODESP emitirá o termo de aceite para os serviços de Assessment e Licenciamento de Devices, após a entrega de relatório técnico e operacional pela CONTRATADA com as evidências dos serviços executados e apresentação dos entregáveis e respectivos resultados no 1º dia útil do mês subsequente a prestação do serviço.

8.2.3.1. O Relatório técnico e operacional deve conter, no mínimo:

I - a quantidade total de *endpoints* efetivamente monitorados no período; e

II - a classificação dos *endpoints* por categoria ou tipo de dispositivo;

8.2.3.2. Os relatórios terão como finalidade garantir transparência na medição do consumo, rastreabilidade contratual, suporte à governança de tecnologia e segurança da informação, bem como subsidiar o acompanhamento da evolução do ambiente tecnológico da PRODESP.

8.2.4. O prazo máximo para emissão do Termo de Aceite do serviço é de 15 dias, a contar da execução do serviço pela CONTRATADA. Caso o serviço não atenda às especificações técnicas, o prazo de aceite será reiniciado após a solução dos problemas detectados.

8.2.5. O prazo máximo para a CONTRATADA solucionar os problemas reportados é de 10 dias a contar do comunicado da PRODESP.

8.3. Níveis Mínimos de Serviço:

8.3.1. Para definição desta contratação, considera-se Nível Mínimo de Serviços (NMS) os parâmetros tangíveis e objetivamente observáveis dos níveis esperados de qualidade na prestação de serviço, bem como respectivas adequações de pagamento.

8.3.2. A PRODESP fará o controle qualitativo da execução contratual por meio dos níveis de serviço definidos abaixo:

NMS	Incide sobre	Nível Mínimo de Serviço (NMS)	Fórmula para Determinação do Impacto por não cumprimento do NMS	Penalidade

Atraso no prazo de entrega estabelecido no Contrato	Valor do Contrato	Cumprir o prazo de entrega constante no Relatório de Projeto de Implantação	Dias úteis de atraso na entrega, conforme o prazo definido no Relatório de Projeto de Implantação	1% (um por cento) para cada dia útil de atraso na entrega, limitado a 15% (quinze por cento) do valor do Contrato
Qualidade dos Serviços executados no Contrato	Valor do Contrato	Entregar o Serviço sem erros	Número de erros técnicos vinculados à execução do Serviço vinculados à execução do serviço	0,5% (cinco décimos por cento) para cada atividade não cumprida totalmente, limitado a 10% (dez por cento) do valor do Contrato
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 1 (Crítico)	Valor da Subscrição SaaS mensal	Prazo de solução em até 4 (quatro) horas	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 da Subscrição mensal
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 2 (Importante)	Valor da Subscrição SaaS mensal	Prazo de solução em até 8 (oito) horas	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 da Subscrição mensal
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 3 (Menor)	Valor da Subscrição SaaS mensal	Prazo de solução em até 2 (dois) 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 da Subscrição mensal
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 4 (Leve)	Valor da Subscrição SaaS mensal	Prazo de solução em até 3 (três) 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 da Subscrição mensal

8.3.3. A CONTRATADA deverá disponibilizar solução de gerenciamento, ou alternativa para acesso aos recursos de gerenciamento e auditoria, tais como API's (*Application Programming Interface*), que permitam à PRODESP aferir os NMS e acompanhar o consumo dos serviços contratados

8.3.4. A CONTRATADA deverá garantir a disponibilidade do acesso a plataforma 24 horas nos 7 dias da semana.

9. DEVERES E RESPONSABILIDADE DA PRODESP

9.1. O tópico constará da minuta de contrato anexa ao Edital.

10. DEVERES E RESPONSABILIDADE DA CONTRATADA

10.1. O tópico constará da minuta de contrato anexa ao Edital.

11. CONDIÇÕES COMERCIAIS E PAGAMENTOS

11.1. Os pagamentos serão efetuados conforme condições abaixo:

11.1.1. **Plataforma de Governança e Maturidade em Cibersegurança:** será paga em 12 parcelas mensais iguais e consecutivas, mediante a disponibilização da plataforma pela CONTRATADA, emissão do termo de aceite e entrega das respectivas Notas Fiscais/Fatura e a devida atestação.

11.2. **Assessment:** será pago mensalmente, mediante a conclusão do serviço, a entrega do relatório técnico mensal de que trata o item 8.2.3, emissão do termo de aceite e entrega das respectivas Notas Fiscais/Fatura e a devida atestação de fatura.

11.3. **Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede):** será paga em 12 parcelas mensais iguais e consecutivas, mediante a conclusão do serviço, a entrega do relatório técnico mensal de que trata o item 8.2.3, emissão do termo de aceite e entrega das respectivas Notas Fiscais/Fatura e a devida atestação de fatura.

11.4. **Serviço de Setup/Implantação:** será pago em parcela única, mediante a conclusão do serviço, emissão do termo de aceite e a entrega das respectivas Notas Fiscais/Fatura e a devida atestação.

11.5. **Serviço de Suporte/Manutenção e Serviço Mensal:** serão pagos mensalmente, mediante a emissão do termo de aceite e entrega das respectivas Notas Fiscais/Fatura e a devida atestação.

11.6. **Serviço de Transferência de Conhecimento (*Hands On*):** será pago após sua conclusão, mediante a entrega da respectiva Nota Fiscal/Fatura e a devida atestação de fatura.

11.7. Nos casos em que os produtos, documentos e serviços entregues não estejam em conformidade com o solicitado ou apresentem defeitos de funcionamento, ou ainda, estejam incompletos, os pagamentos serão suspensos até que os problemas sejam integralmente sanados pela CONTRATADA, conforme a criticidade do problema, caberá a PRODESP a aplicação de penalidades e sanções.

12. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

12.1. Todos os serviços necessários à implantação e entrada em funcionamento da Plataforma, deverão ser entregues em até **30 (trinta) dias corridos** a contar da data da aceitação do Relatório do projeto de implantação conforme as condições estabelecidas neste Termo de Referência.

12.2. Os serviços serão previamente homologados pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

12.3. O recebimento provisório ou definitivo do serviço não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

13. PROPRIEDADE INTELECTUAL

13.1. A PRODESP respeitará o direito de propriedade intelectual da CONTRATADA, consubstanciado no direito autoral, patrimonial e comercial, sobre o sistema contratado, seus componentes de software, suas adaptações, derivações e customizações resultantes da execução dos serviços objeto desta proposta, conforme previsto no texto legal regulamentado pelas Leis n.º 9.609/98 e n.º 9.610/98.

13.2. A PRODESP estará autorizada a disponibilizar o sistema para uso em seus clientes, vedado compartilhar, sublicenciar, vender, ceder ou transferir, onerosa ou não, arrendar, modificar, alugar, transmitir o sistema, bem como deixá-lo disponível em qualquer tipo de serviço online, disponibilizá-lo a qualquer outro órgão sem a prévia autorização por escrito da CONTRATADA.

13.3. Exclusivamente em casos de falência, dissolução total, liquidação ou descontinuidade do sistema pela CONTRATADA, fica assegurado a PRODESP o acesso aos artefatos relacionados e criados durante a execução do contrato, visando garantir a manutenção do referido sistema exclusivamente com equipe técnica própria, não podendo fazê-la por terceiros.

14. SIGILO

14.1. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados e informações contidos em documentos e em mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela PRODESP a tais documentos.

14.2. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da PRODESP.

14.3. A CONTRATADA deverá assegurar o sigilo das informações, documentos e bancos de dados da PRODESP, e adotar todas as providências necessárias para garantir sigilo de toda e qualquer informação a que ver acesso em função da prestação dos serviços previstos neste TR, respondendo administrativa, civil e penalmente por qualquer violação desse preceito;

14.4. A CONTRATADA deverá colaborar com procedimentos de investigação ou auditoria, em especial os em face do uso indevido das informações disponibilizadas para a execução das atividades;

14.5. Todo o material, documentos, softwares, códigos, tecnologias, know-how e demais propriedades intelectuais fornecidas pela PRODESP ou desenvolvidos durante a execução dos serviços de TI são de exclusiva propriedade desta última;

14.6. Em caso de qualquer violação de sigilo ou uso indevido da propriedade intelectual da PRODESP por parte dos profissionais alocados da CONTRATADA, esta será inteiramente responsável pelas consequências legais, administrativas e financeiras decorrentes de tais ações;

14.7. A PRODESP reserva-se o direito de, a qualquer momento, solicitar à CONTRATADA a substituição de qualquer profissional alocado que esteja envolvido em

violação de propriedade intelectual ou outras condutas inadequadas relacionadas aos serviços prestados;

14.8. A responsabilidade da CONTRATADA em relação à proteção de propriedade intelectual sobreviverá à rescisão ou término deste contrato, permanecendo válidas e vinculantes as obrigações de sigilo e confidencialidade durante o período de vigência contratual e mesmo após o seu encerramento.

15. NORMAS, PARÂMETROS E RESPONSABILIDADES DE PROTEÇÃO DE DADOS

15.1. Os serviços a serem contratados deverão observar as normas técnicas, a legislação aplicável e pertinente à celebração de contratos do Poder Público, bem como as normas e diretrizes à Proteção de Dados, sob pena de aplicação das penalidades constantes da lei e do contrato.

15.2. Como parâmetros mínimos de referência para execução dos serviços, e em observância ao atendimento aos padrões de qualidade, objeto do contrato e dos serviços prestados pela PRODESP, deverão ser observadas as seguintes premissas:

15.2.1. Segurança da Informação;

15.2.2. Proteção dos Dados, considerando os fundamentos básicos de respeito à privacidade, autodeterminação informativa, inviolabilidade da intimidade, honra e imagem.

15.3. A CONTRATADA se obriga ao cumprimento das seguintes condições e medidas de Segurança da Informação:

15.3.1. Adotar todas as medidas de segurança, sejam elas técnicas e/ou administrativas objetivando a proteção, privacidade e sigilo dos dados e informações à que tiver acesso, durante todo o contrato, bem como durante o ciclo operacional de serviços prestados, desde a coleta, tratamento e descarte dos dados, incluindo o armazenamento, comunicação e sistemas utilizados, acidentais ou ilícitos como destruição, perda, alteração ou qualquer outra forma inadequada ou ilícita;

15.3.2. Comunicar à PRODESP qualquer ocorrência e/ou incidente de segurança que possa comprometer ou acarretar risco e, danos aos dados tratados;

15.3.3. Não compartilhar ou comercializar qualquer dado ou informação obtidos em decorrência da prestação de serviços, sem a expressa e formal autorização da PRODESP;

15.3.4. Observar e seguir todas as orientações e procedimentos acordados com a PRODESP, não realizando nenhum tratamento que não esteja expressa e previamente autorizado, não coletando nenhum dado ou informação, além do expressamente autorizado;

15.3.5. Ao término do tratamento que envolve a operação de que trata a prestação de serviços contratados, descartar os dados coletados de maneira segura, de sorte a impedir que ocorra sua recuperação;

15.3.6. A CONTRATADA deverá disponibilizar evidências técnicas e/ou relatórios de auditoria que comprovem a aplicação das medidas de segurança descritas nesta cláusula, sempre que solicitado pela PRODESP;

15.3.7. A CONTRATADA assume integral responsabilidade legal, seja civil, penal e/ou administrativa, por eventuais danos materiais e/ou pessoais que forem causados à PRODESP, ao Governo do Estado de SÃO PAULO ou a terceiros, caso não seja observada e cumprida qualquer obrigação assumida no Contrato e seus anexos, bem como na legislação brasileira de Proteção de Dados;

15.3.8. A CONTRATADA assume, além das responsabilidades previstas no Contrato, o uso responsável das informações a que tiver acesso, zelando pela sua segurança e confidencialidade, de forma a garantir o direito à privacidade de seus proprietários.

15.3.9. O descumprimento às obrigações previstas no Contrato e a infringência a qualquer disposição de Proteção de Dados, implicará na responsabilidade da CONTRATADA na assunção das penalidades previstas na legislação vigente.

16. CLÁUSULA DE RESPONSABILIDADE E GARANTIA EM SOLUÇÕES COM INTELIGÊNCIA ARTIFICIAL

16.1. Responsabilidade Técnica e Legal da CONTRATADA:

16.1.1. A CONTRATADA declara que a solução contratada possui componentes de Inteligência Artificial (IA) embarcados, desenvolvidos em conformidade com os princípios legais, éticos e técnicos aplicáveis, incluindo, mas não se limitando, à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), ao Marco Civil da Internet (Lei nº 12.965/2014). A CONTRATADA assume integral responsabilidade por quaisquer falhas, omissões, vícios ocultos, decisões automatizadas indevidas ou danos decorrentes do funcionamento da IA, inclusive aqueles que venham a se manifestar após a entrega da solução.

16.2. Garantia de Conformidade, Disponibilidade e Suporte Técnico:

16.2.1. A CONTRATADA compromete-se a prestar garantia integral e disponibilidade da solução pelo prazo vigente do contrato, contados a partir da data de aceite técnico, abrangendo correções de falhas, atualizações de segurança, mitigação de vieses algorítmicos e suporte técnico especializado. A correção de falhas críticas deverá ocorrer no prazo máximo de 04 (quatro) horas (Conforme Tabela NMS – Item 8.3.2) após a notificação formal da PRODESP.

16.3. Transparência e Explicabilidade:

16.3.1. A CONTRATADA garante que os modelos de IA embarcados na solução possuem mecanismos de auditabilidade, rastreabilidade e explicabilidade, permitindo a PRODESP compreender os critérios utilizados nas decisões automatizadas, bem como contestá-las, quando necessário.

16.4. Mitigação de Riscos e Supervisão Humana:

16.4.1. A solução deverá conter salvaguardas técnicas que permitam supervisão humana sobre decisões automatizadas, especialmente aquelas que possam impactar direitos fundamentais, operações críticas ou relações contratuais. A CONTRATADA deverá implementar mecanismos de controle que permitam a PRODESP intervir ou desativar funcionalidades da IA em caso de risco iminente ou comportamento indevido.

16.5. Continuidade Operacional e Portabilidade:

16.5.1. Em caso de rescisão contratual, a CONTRATADA deverá assegurar a continuidade operacional da solução por um período de transição de 30 (trinta) dias, bem como a portabilidade dos dados e configurações técnicas, em formato interoperável, sem ônus adicional a PRODESP.

17. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

17.1. Regime, Tipo e Modalidade da Licitação

17.1.1. 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 licitação, na modalidade pregão, em sua forma eletrônica, com julgamento pelo critério de MENOR VALOR GLOBAL sobre as condições comerciais, a ser aplicado individualmente sobre cada produto e/ou serviço contemplado no presente Termo de Referência – **ANEXO I-B - PROPOSTA.**

17.2. Participação de Consórcios

17.2.1. A presente contratação não prevê a participação de empresas reunidas em consórcio, uma vez que o objeto licitado não contempla a prestação de serviços/fornecimento de bens de ramos de conhecimentos distintos especializados, na verdade os produtos e serviços são de um único fabricante, ou seja, uma única empresa detém em seu portfólio de serviço condições de atender as demandas prevista nesse Termo de Referência, sem a necessidade de se consorciar com outra empresa para conseguir atender o objeto na sua completude. Desse modo, considerando as características do objeto, não será admitida a participação de consórcios.

17.3. Da admissibilidade de subcontratação

17.3.1. Não será admitida a subcontratação do objeto licitatório.

17.4. Critérios de Qualificação Técnica para a Habilitação

17.4.1. DECLARAÇÃO DA SOLUÇÃO A SER FORNECIDA

a) Deverá ser obrigatoriamente preenchido o **ANEXO I-A** com os dados indicados do produto e/ou solução ofertada, bem como a documentação técnica da solução (datasheet ou documento similar) que permita evidenciar o atendimento das especificações técnicas do Termo de Referência. A declaração deverá ser assinada pelo representante legal do licitante com carimbo ou identificação da assinatura**.**

b) A CONTRATANTE, a seu exclusivo critério, poderá exigir do licitante provisoriamente classificado em primeiro lugar a realização de teste de homologação, prova de conceito ou procedimento equivalente, com o objetivo de verificar a aderência da solução ofertada às especificações técnicas estabelecidas neste Termo de Referência.

- O teste de que trata esta cláusula será conduzido pela equipe técnica da CONTRATANTE, podendo contar com o apoio do licitante, e consistirá na avaliação prática da solução proposta, com base nos requisitos funcionais e não funcionais definidos neste Termo de Referência.
- Para fins de realização do teste, o licitante deverá disponibilizar, no prazo definido pela CONTRATANTE, ambiente, licenças, equipamentos, documentação técnica e todos os recursos necessários à adequada avaliação da solução.

17.4.2. DECLARAÇÃO DE REVENDA AUTORIZADA

a) Declaração de ciência subscrita por representante legal da licitante, comprometendo-se a apresentar, por ocasião da assinatura do contrato, a comprovação de ser Revenda Autorizada do Fabricante da solução ofertada.

b) A comprovação da condição de Revenda Autorizada do Fabricante, pela licitante, deverá ser efetuada mediante a apresentação de documentos comprobatórios, tais como: contrato, atestado emitido em nome da licitante pelo respectivo fabricante, carta de certificação de parceria, emitidos em nome do licitante pelo fabricante, a ser apresentado à PRODESP, ficando a CONTRATADA sujeita à aplicação de penalidades contratuais em caso de descumprimento.

i. O Fabricante fica isento de apresentar a Comprovação de Revenda Autorizada, para sua participação nesta licitação.

c) Serão aceitos documentos eletrônicos, desde que permitida a comprovação de suas autenticidades através de consulta na internet.

17.4.3. ATESTADO DE CAPACIDADE DE FORNECIMENTO

a) A licitante deverá apresentar atestado(s) de bom desempenho anterior em contratos de mesma natureza, de complexidade tecnológica e operacional igual ou superior, fornecido(s) por pessoa(s) jurídica(s) de direito público ou provado, que especifique(m) em seu objeto necessariamente os tipos de serviços realizados, com indicações das quantidades, prazo contratual, datas de início e término e local da prestação de serviços, contemplando a execução dos serviços elencados abaixo relacionados diretamente ao objeto desta contratação.

Tecnologia/Produto	**Quantidade solicitada no tópico 7 - Estimativa da Demanda**	**Quantidade mínima exigida para habilitação técnica**
Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede)	10.000	1.000

- Atestar que forneceu softwares/plataformas contemplando o licenciamento informado acima, atestando inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais.
- Será aceito o somatório de atestados para fins de comprovação da experiência exigida no subitem anterior.
- Cabe destacar que o quantitativo exigido no quadro acima, para fins de habilitação técnica, está em conformidade com o limite estabelecido na Súmula nº 24 do Tribunal de Contas do Estado de São Paulo (TCESP).

b) O atestado deverá conter a identificação da pessoa jurídica emitente, bem como o nome, o cargo do signatário e o telefone para contato.

c) A PRODESP poderá realizar diligência para averiguação da autenticidade dos atestados.

d) Serão aceitos documentos eletrônicos, desde que permitida a comprovação de suas autenticidades através de consulta na internet.

ANEXO I-A
DECLARAÇÃO DOS PRODUTOS A SEREM FORNECIDOS

....., ... de ..... de 2.026.

À Cia de Processamento de Dados do Estado de São Paulo – PRODESP

Ref.: Pregão Nº. _____/2026

Declaro (amos), sob as penas da lei, que, o(s) produto(s)/modelo(s) ofertado(s) a seguir, para participação nesta licitação, são novos, sem utilização anterior e atende(m) a todas e a cada uma das especificações do Anexo I – **REL.GEX.011/2026**; declaro(amos) também que estou(amos) ciente(s) e concordo(amos) que, a falta de veracidade e a inconformidade do(s) bem(ns) ora ofertado(s) neste Anexo I-A com o bem licitado, detalhadamente, especificado no Anexo I, acarretará a aplicação das penalidades cabíveis, previstas neste Edital/Contrato/Pedido de Compra, multa prevista e suspensão da minha empresa que ficará proibida de participar de licitações/contratações da PRODESP, pelo prazo da lei.

1. Da Solução/Plataforma proposta, informar:

a) Nome do fabricante _____

b) Versão _____

ANEXO I-B

TERMO DE CONFIDENCIALIDADE, SIGILO E USO

A Contratada **.....**, inscrita no CNPJ sob o número ....., com sede na cidade ....., doravante designada Signatária, neste ato representada por **.....**, inscrito(a) no CPF sob o número ....., aceita as regras, condições e obrigações constantes do presente Termo.

1. O objetivo deste Termo de Confidencialidade, Sigilo e Uso é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva e/ou sob controle do Contratante reveladas ao Signatário ou por ele acessadas em função da execução do objeto do contrato PRO.00.....

2. A expressão “informações restritas” abrange toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: dados pessoais, técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, marcas e modelos utilizados, preços e custos, definições e informações mercadológicas, invenções e ideias, vulnerabilidades existentes, outras informações técnicas, financeiras ou comerciais, entre outros.

3. A Signatária compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do Contratante, das informações restritas reveladas ou acessadas.

4. A Signatária compromete-se a não utilizar, de forma diversa da prevista no contrato celebrado com o Contratante, as informações restritas reveladas ou acessadas.

5. A Signatária deverá cuidar para que as informações reveladas ou acessadas fiquem limitadas ao conhecimento próprio.

6. A Signatária obriga-se a informar imediatamente ao Contratante qualquer violação das regras de confidencialidade, sigilo e uso estabelecidas neste Termo de que tenha tomado

conhecimento ou que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

7. A quebra da confidencialidade, do sigilo ou das condições de uso das informações restritas reveladas ou acessadas, por ação ou omissão do Signatário, devidamente comprovada, sem autorização expressa do Contratante, sujeitará a Signatária às consequências legais e sanções cabíveis, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo Contratante, inclusive os de ordem moral, bem como às responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

8. O presente Termo tem natureza irrevogável e irretratável.

9. A Signatária manifesta explícita ciência e se compromete a observar as cláusulas de segurança, privacidade e proteção de dados do Contratante, prevista no Contrato PRO.00..... e seus anexos.

E, por aceitar todas as condições e as obrigações constantes do presente Termo, a Signatária assina o presente Termo.

Taboão da Serra, a data de assinatura deste instrumento corresponde a data da última assinatura digital do(s) representante(s) legal(is).

Nome:

CPF:

CONTRATADA

Taboão da Serra, na data da assinatura digital.

FÁBIO MORETH MARIANO
Gerente Executivo de Negócios, Acordos e Contratos Estratégicos

Documento assinado eletronicamente por **Fabio Moreth Mariano**, **Gerente**, em 01/07/2026, às 14:52, 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 **0112949198** e o código CRC **EF4A114D**.

ANEXO II

MODELO DE PLANILHA DE PROPOSTA

À

CIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO – PRODESP

Ref: PREGÃO ELETRÔNICO PRODESP N° 90036/2026 - Processo n° 359.00000183/2026-11

OBJETO: Contratação de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação, controles de privacidade de dados, nível de conformidade com NIST CSF v2 & AI RMF (Artificial Intelligence Risk Management Framework), NIST SP 800-30 - Avaliação de Risco (Risk Assessments), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS Controls v8 Center for Internet Security, ISO 27001 -Information Security, Cybersecurity and Privacy protection , Cyber Insurance, ISO 27701 -Privacy Information Management, ISO 27005 - Information Security Risk Management, ISSO 22301 - Business continuity management systems, ISO 23894 - Artificial intelligence — Guidance on risk management, apontamento por meio de inteligência artificial das melhores práticas de melhorias/sugestões com integração de ferramentas de segurança da informação e consultoria especializada em cibersegurança, conforme as especificações e exigências descritas no Termo de Referência – Anexo I do Edital.

Para cumprimento do objeto deste Pregão, ofertamos os preços conforme quadro a seguir:

Item	Descrição	Unidade	Condição de Pagamento	Quantidade (A)	Número de Meses (B)	Valor Unitário R$ (C)	Valor Total Do Item R$ (D)
1	Plataforma de Governança e Maturidade em Cibersegurança	Un	Parcela Mensal	1	12		**(D) = (A)x(B)x(C)**
2	Assessment	Un	Parcela Única	8.760	-		**(D) = (A)x(C)**
3	Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede)	Un	Parcela Mensal	10.000	12		**(D) = (A)x(B)x(C)**
4	Serviço de Setup/Implantação	Serviço único	Parcela Única	1	-		**(D) = (A)x(C)**
5	Serviço de Suporte/Manutenção e Serviço Mensal	Serviço mensal	Parcela Mensal	1	12		**(D) = (A)x(B)x(C)**
6	Serviço de Transferência de Conhecimento (*Hands On*) para turmas de até 10 alunos	Turma	Parcela Única	02	-		**(D) = (A)x(C)**

PREÇO GLOBAL **(Este é o valor que será utilizado como critério de julgamento e que deverá ser lançado no sistema do Pregão Eletrônico)**	**R$**

Estamos cientes de que o código do item utilizado nesta licitação serviu tão somente para fins de processamento do Pregão Eletrônico no portal de compras (www.gov.br/compras), não se prestando para identificar o objeto licitado, conforme disposto no item 1.2. do Edital.

Declaramos termos examinado todas as especificações contidas no Edital e Anexos, não havendo quaisquer discrepâncias entre o preço final de nossa proposta e as exigências para o cumprimento do objeto licitado, sendo certo que assumimos total responsabilidade por erros ou omissões existentes em nossa proposta, assim como toda despesa relativa à realização integral do objeto.

_____, _____ de _____ de 2026.

_____
Empresa Licitante

_____
(Nome e assinatura do representante legal, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil)

O prazo de validade desta proposta é de 60 (sessenta) dias, a partir da data de sua apresentação.

ANEXO III

MODELO A QUE SE REFERE O ITEM 4.2.4.1. DO EDITAL

(em papel timbrado da licitante)

Nome completo: _____

RG nº: CPF nº:_____

DECLARO, sob as penas da Lei, que o licitante _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº _____/_____, Processo n° _____/_____:

a) está em situação regular perante o Ministério do Trabalho e Emprego no que se refere a observância do disposto no inciso XXXIII do artigo 7.º da Constituição Federal, na forma do Decreto Estadual nº 42.911/1998;
b) não se enquadra em nenhuma das vedações de participação na licitação do item 2.5 deste Edital;
c) não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do artigo 1° e no inciso III do artigo 5° da Constituição Federal.

(Local e data).

_____

(Nome e assinatura do representante legal, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil)

ANEXO IV

DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA E ATUAÇÃO CONFORME AO MARCO LEGAL ANTICORRUPÇÃO

(em papel timbrado da licitante)

Eu, _____, portador do RG nº _____ e do CPF nº _____, representante legal do licitante _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº _____/_____, Processo n° _____/_____, **DECLARO,** sob as penas da Lei, especialmente o artigo 299 do Código Penal Brasileiro, que:

a) a proposta apresentada foi elaborada de maneira independente e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;
b) a intenção de apresentar a proposta não foi informada ou discutida com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;
c) o licitante não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;
d) o conteúdo da proposta apresentada não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório antes da adjudicação do objeto;
e) o conteúdo da proposta apresentada não foi, no todo ou em parte, informado, discutido ou recebido de qualquer integrante relacionado, direta ou indiretamente, ao órgão licitante antes da abertura oficial das propostas; e
f) o representante legal do licitante está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

DECLARO, ainda, que a pessoa jurídica que represento conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, em atendimento à Lei Federal nº 12.846/ 2013 e ao Decreto Estadual nº 67.301/2022, tais como:

I – prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;
II – comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos em Lei;
III – comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
IV – no tocante a licitações e contratos:
a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
d) fraudar licitação pública ou contrato dela decorrente;
e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;

V – dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

(Local e data).

_____

(Nome e assinatura do representante legal, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil)

ANEXO V

DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

(em papel timbrado da licitante)

ATENÇÃO: ESTA DECLARAÇÃO DEVE SER APRESENTADA APENAS POR LICITANTES QUE SEJAM ME/EPP, NOS TERMOS DO ITEM 4.2.4.3. DO EDITAL.

Eu, _____, portador do RG nº _____ e do CPF nº _____, representante legal do licitante _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº _____/_____, Processo n° _____/_____, **DECLARO,** sob as penas da Lei, o seu enquadramento na condição de Microempresa ou Empresa de Pequeno Porte, nos critérios previstos no artigo 3º da Lei Complementar Federal n° 123/2006, bem como sua não inclusão nas vedações previstas no mesmo diploma legal.

(Local e data).

_____

(Nome e assinatura do representante legal, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil)

ANEXO VI

MODELO DE DECLARAÇÃO
(empresas em recuperação judicial)
(em papel timbrado da licitante)

Ref: **Pregão Eletrônico nº _____/_____**.

Eu.....(*nome completo*), representante legal da empresa.....(*nome da pessoa jurídica*), participante do **Pregão Eletrônico n.º _____/_____**, DECLARO, sob as penas da lei:

Estar ciente de que no momento da assinatura do Contrato deverá apresentar cópia do ato de nomeação do administrador judicial ou se o administrador judicial for pessoa jurídica, o nome do profissional responsável pela condução do processo, e, ainda, declaração, relatório ou documento equivalente do juízo ou do administrador, de que o licitante está cumprindo o plano de recuperação judicial.

.....(*localidade*), ...de.....de.....

_____
(Nome e assinatura do representante legal, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil)
CPF n.º.....

ANEXO VII

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO

(em papel timbrado da licitante)

Pela presente, declaramos sob as penas de Lei, a inexistência de qualquer fato impeditivo que obste a nossa participação ou contratação neste **Pregão Eletrônico n° _____/_____** estando esta empresa absolutamente regular no ponto de vista jurídico, financeiro, fiscal e trabalhista, inclusive perante o INSS/FGTS e em virtude das disposições da Lei federal n° 9.605/98 e Decreto estadual n° 66.819/22.

, de de .

_____

(nome da empresa licitante)

_____

(número do Cadastro Nacional de Pessoa Jurídica-CNPJ)

_____

(Nome e assinatura do representante legal, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil)

ANEXO VIII

MODELO DE DECLARAÇÃO DE CIÊNCIA

(em papel timbrado da licitante)

À

Cia. de Processamento de Dados do Estado de São Paulo – PRODESP

Ref: Pregão Eletrônico nº 90036/2026

Declaramos para os devidos fins, que estamos cientes de que se declarada vencedora, por ocasião da celebração do contrato, nossa empresa comprovará ser Revenda Autorizada do fabricante (_____), nos
Indicar o nome do fabricante do produto ofertado
Termos do item 4.2.4.7.do edital.

_____,_____de_____ de _____.

_____
(nome da empresa licitante)

_____
(Nome e assinatura do representante legal, utilizando Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileiras – ICP Brasil)

ANEXO IX

MINUTA DE CONTRATO

CONTRATAÇÃO DE PLATAFORMA PARA SEGURANÇA CIBERNÉTICA QUE REALIZA AVALIAÇÃO DO NÍVEL DE RISCO CORPORATIVO E TECNOLÓGICO COM MONITORAMENTO DE MATURIDADE E AUDITORIA, GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E CONTROLES DE PRIVACIDADE DE DADOS, FIRMADO ENTRE A COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP E A _____.

PRO.00.MINUTA

Pelo presente contrato, de um lado a **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**, com sede no município de Taboão da Serra, estado de São Paulo, na Rua Agueda Gonçalves n.º 240, inscrita no CNPJ/MF sob n.º 62.577.929/0001-35, doravante designada simplesmente **PRODESP**, e, de outro, _____, com sede na _____ - CEP _____, inscrita no CNPJ/MF sob nº _____, doravante designada simplesmente **CONTRATADA**, representadas neste ato por seus representantes legais ao final designados e assinados, tem entre si, justo e acertado, a contratação de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação e controles de privacidade de dados, mediante as seguintes cláusulas e condições:

I - OBJETO

1.1. Constitui objeto do presente contrato, a contratação de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação, controles de privacidade de dados, nível de conformidade com NIST CSF v2 & AI RMF (*Artificial Intelligence Risk Management Framework*), NIST SP 800-30 - Avaliação de Risco (Risk Assessments), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS Controls v8 Center for Internet Security, ISO 27001 - *Information Security, Cybersecurity and Privacy protection*, *Cyber Insurance*, ISO 27701 - *Privacy Information Management*, ISO 27005 - *Information Security Risk Management*, ISO 22301 - *Business continuity management systems*, ISO 23894 - *Artificial intelligence — Guidance on risk management*, apontamento por meio de inteligência artificial das melhores práticas de melhorias/sugestões com integração de ferramentas de segurança da informação e consultoria especializada em cibersegurança, conforme detalhado no Termo de Referência – Anexo I, e demais condições estabelecidas neste contrato.

1.1.1. A solução de TIC deverá atender os requisitos constantes dos itens 4. DESCRIÇÃO DA SOLUÇÃO DE TIC e 5. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO e respectivos subitens do Termo de Referência – Anexo I.

1.1.2. Os serviços e as quantidades são as constantes do quadro abaixo:

Item	Descrição	Unidade	Quantidade
1	Plataforma de Governança e Maturidade em Cibersegurança - SaaS	Un	01
2	Assessment	Un	8.760
3	Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede)	Un	10.000
4	Serviço de Setup/Implantação	Serviço Único	01
5	Serviço de Suporte/Manutenção e Serviço Mensal	Serviço Mensal	12
6	Serviço de Transferência de Conhecimento (*Hands On*) para turmas de até 10 alunos	Turma	02

1.2. O regime de execução dos serviços objeto deste contrato é de empreitada por preço unitário.

1.3 A presente contratação, decorrente de licitação na modalidade Pregão Eletrônico n.° _____/_____, foi homologada, assim como autorizada a previsão de despesa orçamentária no Documento de Comprovação Orçamentária – DCO nº ____/____, nos termos do Decreto Estadual n.º 33.144, de 20/03/1991, conforme documentos anexados no Processo PRODESP n.º_____.

II – PRESTAÇÃO DOS SERVIÇOS E PRAZOS

2.1. A **CONTRATADA** deverá executar os serviços atendendo as especificações técnicas estabelecidas no Termo de Referência - Anexo I deste contrato.

2.2. O escopo da solução e a especificação dos requisitos do objeto do presente contrato, estão detalhados nos itens 4. DESCRIÇÃO DA SOLUÇÃO DE TIC e 5. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO e respectivos subitens do Termo de Referência – Anexo I deste contrato.

2.3. Após assinatura do contrato, será realizada reunião inicial (kickoff) entre a **PRODESP** e a **CONTRATADA** para alinhamento, definição do cronograma e demais condições, conforme previsto nos itens 5.15.4.2., 5.15.4.10., 6.1. e seus subitens do Termo de Referência – Anexo I. Na data da 1ª reunião à **CONTRATADA** deverá apresentar sua equipe de trabalho, composta pelo Gestor do Projeto e sua Equipe Técnica.

2.4. A **CONTRATADA** deverá entregar, para validação da **PRODESP**, pelo menos, 02 (dois) RELATÓRIOS com conteúdo definidos a seguir:

a) Relatório de Projeto de Implantação (“AS BUILT”):

- Contempla-se neste Relatório, a etapa de planejamento para a implantação do objeto especificado no Termo de Referência – Anexo I;
- O relatório deverá contemplar e detalhar todas as etapas da instalação, isto é, os serviços de planejamento, instalação, integração e pré-operação;
- O relatório deverá contemplar cronograma informando o prazo para a execução de cada etapa do serviço contemplado no Termo de Referência – Anexo I;
- O relatório deverá contemplar a arquitetura desenhada pela **CONTRATADA**;
- O prazo máximo para a entrega do Relatório de Projeto de Implantação pela **CONTRATADA** à **PRODESP** é de 15 (quinze) dias a contar da data da 1ª reunião de acompanhamento da execução do contrato.

b) Relatório Final de Implantação.

- Neste documento deverão constar todas as informações geradas pela **CONTRATAD**A abordando os aspectos da arquitetura implantada, configuração, testes e integração ao ambiente da **PRODESP**.
- O Relatório Final de Implantação deverá ser fornecido no prazo máximo de 15 (quinze) dias a contar da data de conclusão e validação do SERVIÇO DE IMPLANTAÇÃO especificado no Termo de Referência – Anexo I.

2.4.1. Todos os relatórios de projeto "As Built" serão considerados como efetivamente entregues e aceitos somente após a validação pela equipe técnica da **PRODESP** que se fará no prazo máximo de 10 (dez) dias a contar da respectiva entrega.

2.4.1.1. Os relatórios deverão ser apresentados em via impressa e/ou meio digital, conforme acordado entre as partes;

2.4.1.2. O software empregado na confecção dos textos integrantes das documentações deverá ser totalmente compatível com o MS Word em versão mais recente;

2.4.1.3. Os relatórios deverão ser emitidos em papel timbrado da **CONTRATADA** e deverão conter o nome, data e assinatura do Gestor de Projeto da **CONTRATADA**.

2.5. Todos os serviços necessários à implantação e entrada em funcionamento da Plataforma, deverão ser entregues em até **30 (trinta) dias corridos** a contar da data da aceitação do Relatório do Projeto de Implantação, conforme as condições estabelecidas no Termo de Referência – Anexo I deste contrato.

2.5.1. Os serviços serão previamente homologados pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência – Anexo I;

2.5.2. O recebimento provisório ou definitivo do serviço não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

2.6. A **CONTRATADA** deverá cumprir os Requisitos de Manutenção e Suporte Técnico estabelecido no item 5.5. e em seus subitens do Termo de Referência – Anexo I.

2.7. Para o atendimento de chamados técnicos relacionados a sistemas/serviços ofertados pela **CONTRATADA** deverão ser respeitados os prazos de atendimento conforme tabela abaixo:

SLA –*Service Level Aggrement* – Nível de Serviço Aceito

Nível de Severidade	Tipo de Severidade	Descrição do Evento	Tempo para início de atendimento	Tempo para Resposta e Solução a partir do acionamento
Severidade 1 (Crítico)	(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 **PRODESP** alocará um contato durante este período, seja no local ou por telefone, para auxiliar na coleta de dados, testes e aplicação de correções.	01 hora	04 horas (Horário comercial)
Severidade 2 (Importante)	Alta	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 PRODESP não consegue prosseguir com a instalação de qualquer produto contratado, impedindo-o de disponibilizá-lo aos usuários.	02 horas	08 horas (Horário comercial)
Severidade 3 (Menor)	Média	A perda do serviço é pequena, o problema gera inconvenientes que podem exigir uma solução alternativa para restaurar a funcionalidade.	24 horas	48 horas (Horário comercial)
Severidade 4 (Leve)	Baixa	Não há impacto na operação e perda de serviço. O resultado não impede o funcionamento do sistema.	48 horas	72 horas (Horário comercial)

2.8. A **CONTRATADA** pode apresentar uma solução de contorno para o restabelecimento do serviço, até que possa apresentar a solução definitiva.

2.9. A **CONTRATADA** envidará esforços contínuos para solucionar as Solicitações de Serviços de Severidades 1 e 2.

2.10. A **CONTRATADA** iniciará escalonamento interno para as solicitações de Severidade 1 e Severidade 2 de acordo com as Respostas às Solicitações de Serviços.

2.11. A **CONTRATADA** priorizará o reparo de defeitos dos programas envolvidos durante a resolução das solicitações de serviço.

2.12. Todas as subscrições e serviços necessários à implantação e entrada em funcionamento da Plataforma, devem ser disponibilizados conforme os prazos estabelecidos no Termo de Referência – Anexo I.

2.13. Os prazos para início dos serviços de Transferência de Conhecimento (*Hands On*), devem ser definidos mediante acordo entre as partes. A **CONTRATADA** deverá executar os serviços atendendo as condições e prazos estabelecidas no item 6.2. e seus subitens do Termo de Referência – Anexo I.

2.14. As licenças deverão ser entregues acompanhadas de garantias do Fabricante e direito de atualização das versões pelo período contratado, a contar da data de entrega e ativação dos produtos e/ou serviços objeto do presente contrato, conforme condições estabelecidas no subitem 5.11.1. do Termo de Referência – Anexo I.

2.15. Níveis Mínimos de Serviço.

2.15.1. Para definição desta contratação, considera-se Nível Mínimo de Serviços (NMS) os parâmetros tangíveis e objetivamente observáveis dos níveis esperados de qualidade na prestação de serviço, bem como respectivas adequações de pagamento.

2.15.2. A **PRODESP** fará o controle qualitativo da execução contratual por meio dos níveis de serviço definidos abaixo:

NMS	Incide sobre	Nível Mínimo de Serviço (NMS)	Fórmula para Determinação do Impacto por não cumprimento do NMS	Penalidade
Atraso no prazo de entrega estabelecido no Contrato	Valor do Contrato	Cumprir o prazo de entrega constante no Relatório de Projeto de Implantação	Dias úteis de atraso na entrega, conforme o prazo definido no Relatório de Projeto de Implantação	1% (um por cento) para cada dia útil de atraso na entrega, limitado a 15% (quinze por cento) do valor do Contrato
Qualidade dos Serviços executados no Contrato	Valor do Contrato	Entregar o Serviço sem erros	Número de erros técnicos vinculados à execução do Serviço vinculados à execução do serviço	0,5% (cinco décimos por cento) para cada atividade não cumprida totalmente, limitado a 10% (dez por cento) do valor do Contrato
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 1 (Crítico)	Valor da Subscrição SaaS mensal	Prazo de solução em até 4 (quatro) horas	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 da Subscrição mensal
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 2 (Importante)	Valor da Subscrição SaaS mensal	Prazo de solução em até 8 (oito) horas	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 da Subscrição mensal
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 3 (Menor)	Valor da Subscrição SaaS mensal	Prazo de solução em até 2 (dois) 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 da Subscrição mensal
Atraso na Resposta e Solução a partir do acionamento do chamado de Severidade 4 (Leve)	Valor da Subscrição SaaS mensal	Prazo de solução em até 3 (três) 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 da Subscrição mensal

2.16. A **CONTRATADA** deverá disponibilizar solução de gerenciamento, ou alternativa para acesso aos recursos de gerenciamento e auditoria, tais como API's (*Application Programming Interface*), que permitam à **PRODESP** aferir os NMS e acompanhar o consumo dos serviços contratados.

2.17. A **CONTRATADA** deverá garantir a disponibilidade do acesso a plataforma 24 horas nos 7 dias da semana.

III - ACEITE

3.1. A **PRODESP** emitirá o Termo de Aceite da Plataforma, após a constatação de sua implantação/liberação, considerando que os serviços foram executados em conformidade com as especificações técnicas contidas no Termo de Referência - Anexo I, bem como em observância aos Níveis Mínimos de Serviço estabelecidos na tabela do subitem 2.15.2. deste contrato.

3.2. A **PRODESP** emitirá o Termo de Aceite para o serviço de setup/implantação após a instalação da plataforma em ambiente de produção.

3.3. A **PRODESP** emitirá o termo de aceite para os serviços de Assessment e Licenciamento de Devices, após a entrega de relatório técnico e operacional pela **CONTRATADA** com as evidências dos serviços executados e apresentação dos entregáveis e respectivos resultados no 1º dia útil do mês subsequente a prestação do serviço.

3.3.1. O Relatório técnico e operacional deve conter, no mínimo:

I - a quantidade total de endpoints efetivamente monitorados no período; e

II - a classificação dos endpoints por categoria ou tipo de dispositivo;

3.3.2. Os relatórios terão como finalidade garantir transparência na medição do consumo, rastreabilidade contratual, suporte à governança de tecnologia e segurança da informação, bem como subsidiar o acompanhamento da evolução do ambiente tecnológico da **PRODESP**.

3.4. O prazo máximo para emissão do Termo de Aceite do serviço é de 15 (quinze) dias, a contar da execução do serviço pela **CONTRATADA**. Caso o serviço não atenda às especificações técnicas contidas no Termo de Referência - Anexo I, o prazo de aceite será reiniciado após a solução dos problemas detectados.

3.5. O prazo máximo para a **CONTRATADA** solucionar os problemas reportados é de 10 (dez) dias a contar do comunicado da **PRODESP**.

IV – VIGÊNCIA DO CONTRATO

4.1. A vigência do presente contrato é de **12 (doze) meses**, contados a partir da data de sua assinatura, podendo ser prorrogada, mediante acordo entre as partes, até o limite de 05 (cinco) anos, excetuando-se os serviços de Setup/Implantação e de Transferência de Conhecimento (Hands-On), previstos nos itens 4 e 6 do quadro constante do subitem 1.1.2 da Cláusula I – OBJETO.

V – PREÇO E REAJUSTE

5.1. O valor total estimado do presente contrato é de R$ _____ (_____), base: ___/__/____.

5.2. Pelos serviços contratados a **PRODESP** pagará à **CONTRATADA** os seguintes valores:

Plataforma de Governança e Maturidade Cibernética - SaaS					
Item	**Descrição**	**Unidade**	**Qtd.**	**Valor Mensal R$**	**Valor Total para 12 meses R$**
1	Plataforma de Governança e Maturidade em Cibersegurança - SaaS	Un	01		
Item	**Descrição**	**Unidade**	**Qtd.**	**Valor Unitário R$**	**Valor Total R$**
2	Assessment	Un	8.760		
Item	**Descrição**	**Unidade**	**Qtd.**	**Valor Mensal R$**	**Valor Total para 12 meses R$**
3	Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede)	Un	10.000		
Item	**Descrição**	**Unidade**	**Qtd.**	**Valor Unitário R$**	**Valor Total R$**
4	Serviço de Setup / Implantação	Serviço Único	01		
5	Serviço de Suporte/Manutenção e Serviço Mensal	Serviço Mensal	12		
6	Serviço de Transferência de Conhecimento (*Hands On*) para turmas de até 10 alunos	Turma	02		
Valor Total R$					

5.3. No preço estabelecido já estão inclusos todos os custos diretos e indiretos relativos ao seu objeto, abrangendo todas as despesas necessárias para a execução do serviço, inclusive despesas com taxas, materiais, transportes, fretes, mão de obra, bem como todos os benefícios e encargos sociais, trabalhistas, previdenciários, tributários, securitários, ficando todos estes itens sob a responsabilidade da **CONTRATADA**, não cabendo à **PRODESP** arcar com custos adicionais a quaisquer títulos.

5.4. Os valores dos serviços previstos nos itens 1, 2, 3 e 5 do quadro do item 5.2., serão reajustados anualmente, de acordo com a variação do IPC-FIPE (Índice de Preços ao Consumidor) mediante aplicação da seguinte fórmula:

$$R = Po \cdot \left[\left(\frac{IPC}{IPCo} \right) - 1 \right]$$

Onde:

R = parcela de reajuste;

Po = preço inicial do contrato no mês de referência dos preços, ou preço do contrato no mês de aplicação do último reajuste;

IPC/IPCo = variação do IPC FIPE - Índice de Preço ao Consumidor, ocorrida entre o mês de referência de preços, ou o mês do último reajuste aplicado, e o mês de aplicação do reajuste;

5.4.1. Na hipótese de superveniência de disposição da Lei Federal ou de determinação do Poder Executivo Federal, permitindo a aplicação de reajuste de preço em periodicidade inferior à prevista no item 5.4., poderão as partes contratantes repactuar a nova periodicidade, obedecida as condições que a Lei, então vigente, estabelecer.

5.4.2. Na hipótese de suspensão, extinção ou vedação do uso do índice estabelecido no item 5.4., será utilizado o índice oficial que vier a substituí-lo ou, no caso de não determinação deste, será escolhido o índice substituto que melhor venha refletir a variação dos custos da **CONTRATADA**.

5.4.3. Na periodicidade prevista no item 5.4. e de acordo com o percentual máximo de reajuste apurado nos termos do mencionado item, as partes negociarão o percentual a ser aplicado sobre o valor do presente contrato, a título de reajuste, fundamentado em planilhas de custo ou outros documentos que comprovem o pleito da **CONTRATADA**.

5.5. Caso a **CONTRATADA** seja optante pelo Simples Nacional e, por causa superveniente à contratação, perca as condições de enquadramento como microempresa ou empresa de pequeno porte ou, ainda, torne-se impedida de beneficiar-se desse regime tributário diferenciado por incorrer em alguma das vedações previstas na Lei Complementar Federal nº 123/2006, não poderá deixar de cumprir as obrigações avençadas perante a Administração, tampouco requerer o reequilíbrio econômico-financeiro, com base na alegação de que a sua proposta levou em consideração as vantagens daquele regime tributário diferenciado.

5.5.1. No caso de tornar-se impedida de beneficiar-se do Simples Nacional, a **CONTRATADA** deverá requerer ao órgão competente a sua exclusão do Simples Nacional até o último dia útil do mês subsequente àquele em que foi celebrado o contrato, nos termos do artigo 30, caput, inciso II, e §1º, inciso II, da Lei Complementar Federal nº 123/2006, apresentando à **PRODESP** a comprovação da exclusão ou o seu respectivo protocolo.

VI - FATURAMENTO E PAGAMENTO

6.1. O faturamento do objeto do presente contrato deverá ser feito no CNPJ da **PRODESP**, correspondente ao local de entrega e/ou da prestação dos serviços. Para tanto, a **CONTRATADA** deverá consultar os dados cadastrais

correspondentes, no endereço eletrônico: www.prodesp.sp.gov.br/fornecedores/filiais-prodesp.

6.2. As Notas Fiscais/Faturas representativas dos pagamentos deverão ser emitidas pela CONTRATADA contra a PRODESP e enviadas eletronicamente em formato e nomenclatura padrão estabelecida no manual de instruções disponível no site da PRODESP, www.prodesp.sp.gov.br, na seção “Fornecedores” opção “Entrega de Notas Fiscais e Faturas”.

6.2.1. A **PRODESP**, na qualidade de empresa pública integrante da Administração Indireta, observará, para fins de retenção tributária, o disposto no Regulamento do Imposto de Renda (RIR/2018) quanto ao IRRF, bem como a Lei nº 10.833/2003 no que se refere às retenções de PIS, COFINS e CSLL.

6.2.2. O endereço eletrônico informado no item acima destina-se exclusivamente ao recebimento de Nota Fiscal Eletrônica e não será aceito o envio por e-mail. A entrega de quaisquer outros documentos exigidos deverá seguir o estabelecido com a **PRODESP**.

6.2.3. As notas fiscais e faturas devem ser emitidas e entregues até o dia 25 do mês subsequente ao da prestação do serviço.

6.2.4. Na hipótese de divergência entre os valores constantes na Nota Fiscal/Fatura emitida pela **CONTRATADA** e o estipulado no contrato ou nas medições, a **PRODESP** poderá glosar os valores apontados como indevidos.

6.2.5. A **PRODESP** tem a obrigação de assegurar que todos os aspectos fiscais e tributários estejam em conformidade com a legislação vigente. Caso haja alguma inconsistência ou dúvida quanto ao enquadramento tributário do documento fiscal emitido, a **PRODESP** poderá reter o pagamento até que a situação seja esclarecida ou regularizada.

6.3. Os pagamentos, cumpridas as condições acima, serão efetuados pela **PRODESP** na forma dos itens 6.4. e 6.5., respeitando o quanto disposto no item 6.7. desta cláusula.

6.3.1. Havendo atraso nos pagamentos, incidirá correção monetária sobre o valor devido na forma da legislação aplicável, bem como juros moratórios, a razão de 0,5% (meio por cento) ao mês, calculados pro rata temporis, em relação ao atraso verificado.

6.4. Os pagamentos pelos serviços prestados e aceitos, e em conformidade com o(s) preço(s) estabelecido(s) no item 5.2. deste contrato, serão efetuados pela **PRODESP**, após o recebimento das respectivas notas fiscais/faturas e a devida atestação pela **PRODESP**, mediante as seguintes condições:

6.4.1. **Plataforma de Governança e Maturidade em Cibersegurança - SaaS:** será paga em 12 parcelas mensais iguais e consecutivas, mediante a disponibilização da plataforma pela **CONTRATADA**, emissão do termo de

aceite e entrega da(s) respectiva(s) Nota(s) Fiscal(is)/Fatura(s) e a devida atestação de fatura.

6.4.2. **Assessment:** será pago mensalmente, mediante a conclusão do serviço, a entrega do relatório técnico mensal de que trata o item 3.3. deste contrato, emissão do termo de aceite e entrega da(s) respectiva(s) Nota(s) Fiscal(is)/Fatura(s) e a devida atestação de fatura.

6.4.3. **Licenciamento de Devices (Servidores, Notebooks, Desktops e ativos de rede):** será paga em 12 parcelas mensais iguais e consecutivas, mediante a conclusão do serviço, a entrega do relatório técnico mensal de que trata o item 3.3. deste contrato, emissão do termo de aceite e entrega das respectivas Notas Fiscais/Fatura e a devida atestação de fatura.

6.4.4. **Serviço de Setup/Implantação:** será pago em parcela única, mediante a conclusão do serviço, emissão do termo de aceite e a entrega da(s) respectiva(s) Nota(s) Fiscal(is)/Fatura(s) e a devida atestação de fatura.

6.4.5. **Serviço de Suporte/Manutenção e Serviço Mensal:** serão pagos mensalmente, mediante a emissão do termo de aceite e entrega da(s) respectiva(s) Nota(s) Fiscal(is)/Fatura(s) e a devida atestação de fatura.

6.4.6. **Serviço de Transferência de Conhecimento (*Hands On*):** será pago após conclusão dos serviços, mediante a entrega da(s) respectiva(s) Nota(s) Fiscal(is)/Fatura(s) e a devida atestação de fatura.

6.5. Todos os pagamentos previstos no item 6.4. deverão observar as regras estabelecidas abaixo:

6.5.1. A **PRODESP** realizará pagamentos nos dias 5 e 20 do mês, sendo prorrogados para o dia útil subsequente, no caso de dias não úteis;

6.5.2. As Notas Fiscais/Faturas entregues pela **CONTRATADA** entre os dias 1 e 5 do mês subsequente à prestação dos serviços serão pagas no dia 5 do mês subsequente à entrega. As Notas Fiscais/Faturas entregues após o dia 5, serão pagas no dia 20 do mês subsequente à entrega. As Notas Fiscais/Faturas entregues após o dia 21, serão pagas no dia 5 do mês subsequente, fora o mês de sua entrega.

6.5.3. No caso de devolução de Nota Fiscal/Fatura por qualquer motivo, a reapresentação será considerada como nova solicitação para efeito de contagem do prazo de seu pagamento.

6.5.4. Nos casos em que os produtos, documentos e serviços entregues não estejam em conformidade com o solicitado ou apresentem defeitos de funcionamento ou ainda, estejam incompletos, os pagamentos serão suspensos até que os problemas sejam integralmente sanados pela **CONTRATADA**. Conforme a criticidade do problema, caberá à **PRODESP** a aplicação de penalidades.

6.6. As importâncias a serem pagas pela **PRODESP** serão depositadas em conta corrente da **CONTRATADA** no Banco do Brasil S.A.

6.6.1. Para tanto, a **CONTRATADA** deverá informar à **PRODESP**, dentro do prazo de 15 (quinze) dias corridos a contar da assinatura do presente contrato, o número de sua conta corrente e o da agência do referido estabelecimento bancário.

6.7. Constitui condição para a realização dos pagamentos a inexistência de registros em nome da **CONTRATADA** 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, pela **CONTRATADA**, de que os registros estão suspensos, nos termos do artigo 8° da Lei Estadual n° 12.799/2008.

6.8. A **PRODESP** efetuará a retenção/recolhimento referente ao INSS, conforme previsto na Lei Federal n.º 9.711/98 de 20/11/98 e do percentual relativo ao ISSQN nos termos da Lei Complementar n.º 116/2003, se aplicáveis.

6.9. Todos os tributos sejam eles, federais, estaduais ou municipais sob qualquer título, inclusive o I.S.S. (Imposto Sobre Serviços) que incidam ou venham a incidir sobre este contrato são de exclusiva responsabilidade da **CONTRATADA**.

6.10. A **PRODESP** reserva-se o direito de solicitar à **CONTRATADA**, quando entender conveniente, a exibição dos comprovantes de recolhimento dos tributos e demais encargos devidos, diretos ou indiretamente, a respeito deste contrato.

6.11. É assegurado à **PRODESP** efetuar, nos termos do artigo 70 do seu Regulamento Interno de Licitações e Contratos, a retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, quando a **CONTRATADA**:

a) não produzir os resultados, deixar de executar, ou não executar com a qualidade exigida as atividades contratadas;

b) deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com quantidade inferior à demandada;

c) estiver sendo processado judicialmente pelo descumprimento de obrigações trabalhistas e previdenciárias dos seus empregados, decorrentes da execução do contrato, em tendo sido a **PRODESP** incluída no polo passivo da ação.

6.12. Quando da emissão da nota fiscal, caso a **CONTRATADA** esteja em situação de recuperação judicial, deverá apresentar declaração, relatório ou documento equivalente de seu administrador judicial, ou se o administrador judicial for pessoa jurídica, do profissional responsável pela condução do processo, de que está cumprindo o plano de recuperação judicial.

6.12.1. A não apresentação do documento requerido no item 6.12. acarretará a aplicação de multa prevista na cláusula XIV - RESCISÃO E PENALIDADES.

6.13. A **CONTRATADA**, optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições (SIMPLES) junto à Secretaria da Receita Federal (SRF), nos termos da Lei Complementar nº 123, de 14 de dezembro de 2006, deverá apresentar a cada

pagamento, nos termos do anexo da Instrução Normativa n.º 791 de 10 de dezembro de 2007 da Secretaria da Receita Federal (SRF), DECLARAÇÃO, emitida em duas vias e devidamente assinadas pelo representante legal da **CONTRATADA**. A não apresentação da respectiva declaração ensejará a retenção na fonte dos tributos e contribuições devidos.

6.13.1. A **PRODESP** arquivará a primeira via da declaração a que se refere o item acima, que ficará à disposição da Secretaria da Receita Federal (SRF), devendo a segunda via ser devolvida à **CONTRATADA**, como recibo.

VII – GARANTIA DE EXECUÇÃO CONTRATUAL

7.1. Para garantir o fiel cumprimento de todas as obrigações assumidas no presente contrato, a **CONTRATADA** deverá, no prazo máximo de 15 (quinze) dias úteis, prorrogável por igual período, a critério da **PRODESP**, contado da assinatura deste contrato, fornecer garantia de execução contratual equivalente a 5% (cinco por cento) do valor deste Contrato, com validade que abranja todo o período contratual.

7.2. A garantia mencionada no item 7.1. será prestada por caução em dinheiro, seguro-garantia ou fiança bancária.

7.2.1. A caução em dinheiro deve ser emitida sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

7.2.2. Não será aceita carta de fiança emitida por sociedade não registrada como instituição financeira junto ao Banco Central do Brasil, conforme Parecer SubG Cons. Nº 63/2016 da Procuradoria Geral do Estado de São Paulo;

7.2.3. A garantia mencionada nos itens 7.1 e 7.2., deverá ser válida por prazo não inferior à vigência do contrato ou de suas prorrogações, devendo ser providenciada, sempre que necessária, a sua revalidação.

7.3. A **CONTRATADA** providenciará complementação da garantia, de forma a manter a equivalência estipulada no item 7.1., no prazo máximo de 15 (quinze) dias úteis, contado da assinatura de eventual aditamento que altere o valor deste contrato.

7.4. A inobservância do prazo fixado para apresentar a garantia ou a sua complementação, conforme disposto nos itens 7.1. e 7.3. acarretará aplicação de multa prevista na Cláusula XIV – RESCISÃO E PENALIDADES.

7.4.1. O atraso superior a 25 (vinte e cinco) dias autorizará a **PRODESP** a:

a) promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas obrigações, ou

b) reter o valor dos pagamentos eventualmente devidos ao contratado, até que a garantia seja apresentada.

7.4.2. A **PRODESP** devolverá à **CONTRATADA** o valor retido, sem juros, correção monetária, ou qualquer outro acréscimo, em até 10 (dez) dias úteis, após a data de apresentação ou complementação da garantia.

7.5. A garantia de execução assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

7.5.1. Prejuízos advindos do inadimplemento total ou parcial do objeto do contrato;

7.5.2. Prejuízos diretos causados à **PRODESP** decorrentes de culpa ou dolo da **CONTRATADA** durante a execução do objeto do contrato;

7.5.3. Multas, moratórias e compensatórias, aplicadas pela **PRODESP** à **CONTRATADA**; e

7.5.4. Obrigações trabalhistas e previdenciárias relacionadas ao contrato **não** adimplidas pela **CONTRATADA**.

7.6. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as seguintes:

7.6.1. Caso fortuito ou força maior;

7.6.2. Descumprimento das obrigações pela **CONTRATADA** decorrentes de atos ou fatos imputáveis exclusivamente à **PRODESP**.

7.7. A garantia prestada pelo contratado será liberada ou restituída, após a execução de todas as obrigações contratuais, devendo ser atualizada monetariamente na hipótese de caução em dinheiro pelo IPC FIPE – Índice de Preço ao Consumidor ou no caso de sua extinção, pelo índice previsto na legislação estadual aplicável, vigente na data da devolução e calculada desde a data de sua prestação.

7.8. A qualquer tempo, a **PRODESP** poderá, justificadamente, exigir a substituição da garantia ofertada, devendo ser atendida no prazo máximo de 15 (quinze) dias úteis.

7.9. A garantia deve assegurar a cobertura de todos os eventos ocorridos durante a sua validade, ainda que o sinistro seja comunicado pela **PRODESP** após expirada a vigência do contrato ou a validade da garantia.

VIII - OBRIGAÇÕES DA CONTRATADA

8.1. Executar o objeto contratado, cumprindo, rigorosamente, todas as suas cláusulas, condições e prazos, inclusive os previstos no seu Termo de Referência – Anexo I, durante toda a sua vigência.

8.2. Prestar todas as informações e esclarecimentos necessários ao acompanhamento dos trabalhos, sempre que solicitado.

8.3. Conduzir os trabalhos de acordo com as normas técnicas adequadas, em estrita observância às normas legais aplicáveis.

8.4. Garantir que qualquer serviço contratado será executado por profissionais qualificados e especializados, em conformidade com o estabelecido no Anexo I.

8.5. Responsabilizar-se integralmente pela qualidade técnica dos trabalhos por ela desenvolvidos.

8.6. Assumir toda responsabilidade pelos danos que eventualmente venham a ser causados por seus empregados ou prepostos na prestação dos serviços objeto do presente contrato.

8.7. Permitir e facilitar que a **PRODESP**, através de um funcionário por ela indicado, inspecione a qualquer tempo a execução dos trabalhos, devendo prestar todas as informações e esclarecimentos solicitados.

8.8. Obriga-se, por seus administradores, sócios e gerentes, por seus funcionários ou terceiros contratados e/ou subcontratados, credenciados e representantes, a manter e guardar o mais expresso, estrito e absoluto sigilo sobre dados, informações, conteúdo, especificações técnicas, características de ambientes, relações ou informações de caráter comercial com clientes da **PRODESP**, a que tenham acesso ou conhecimento, sob qualquer forma, em decorrência da prestação dos serviços e/ou fornecimento de bem, objeto deste contrato, no decorrer da sua execução ou cumprimento, sob pena de responder civil ou criminalmente pelo seu descumprimento, ficando responsável pela reparação por prejuízos materiais, morais, perdas e lucros cessantes decorrentes.

8.8.1. A obrigação de sigilo prevista no item 8.8., aplica-se não só pelo prazo de vigência ou de execução dos serviços/fornecimento previstos neste contrato como se estende também após seu encerramento pelo prazo de 10 (dez) anos.

8.9. Não emitir e/ou fazer circular duplicatas ou saque de letras de câmbio contra a **PRODESP**, relativamente a todo e qualquer crédito decorrente deste contrato, exceto em se tratando a **CONTRATADA** de microempresa ou empresa de pequeno porte.

8.10. Responsabilizar-se, sem qualquer espécie de solidariedade por parte da **PRODESP**, pelas obrigações de natureza fiscal, previdenciária, trabalhista, acidentária e civil, em relação ao pessoal que alocar para a prestação dos serviços objeto do presente contrato.

8.10.1. Apresentar à **PRODESP**, quando exigido, comprovante de pagamento de salários, apólices de seguros, quitação de suas obrigações trabalhistas e previdenciárias, relativas aos seus empregados que estejam ou tenham estado a serviço da **PRODESP**, por força deste contrato.

8.11. Obedecer na execução e desenvolvimento do seu trabalho, as determinações da Lei n.º 6.514, de 22 de dezembro de 1977, regulamentada pela Portaria n.º 3.214, de 08 de junho de 1978, do Ministério do Trabalho e Emprego e suas alterações, além de outra legislação técnica vigente e as normas de procedimentos internos da **PRODESP**, de engenharia de segurança, medicina e meio ambiente do trabalho, que sejam aplicáveis à execução específica da atividade.

8.12. Observada a natureza do objeto contratado, responsabilizar-se exclusivamente, pela retirada e descarte do material até o destino final, sempre que solicitado pela **PRODESP**, obrigando-se a apresentar a documentação comprobatória de sua qualificação para tanto, de conformidade com a legislação pertinente, sob pena de rescisão do ajuste, bem como da imposição das penalidades nele previstas.

8.13. Apresentar, sempre que solicitado pela **PRODESP**, cópia dos Programas de Controle Médico de Saúde Ocupacional – PCMSO e Programa de Gerenciamento de Riscos - PGR, de acordo com as Normas Regulamentadoras n.ºs 07 e 09, respectivamente, da Portaria n.º 3.214, de 08 de junho de 1978, do Ministério do Trabalho e Emprego, conforme determina a Lei Federal n.º 6.514, de 22 de dezembro de 1977 e instalando e mantendo os Serviços Especializados em Engenharia de Segurança e em Medicina do Trabalho (SEESMT) e Comissão Interna de Prevenção de Acidentes – CIPA, considerando o número total de trabalhadores nos serviços, para o fiel cumprimento da legislação em vigor.

8.14. Providenciar, concomitantemente à assinatura do contrato, seu cadastro na Unidade Cadastradora do SICAF, ou sua renovação, caso esteja com o cadastro vencido, bem como mantê-lo válido durante toda vigência contratual.

8.15. Manter, nos termos do artigo 69, Inciso IX da Lei Federal nº 13.303/2016, durante toda a execução deste contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

8.15.1. A **CONTRATADA** deverá comunicar imediatamente ao Gestor do Contrato da **PRODESP** a ocorrência de superveniência ou fato que venha a modificar suas condições iniciais de habilitação e qualificação.

8.15.2. A **PRODESP** promoverá consulta da regularidade das certidões e cadastros, no ato de assinatura do contrato e previamente à emissão de termo de aditamento, por meio dos sistemas eletrônicos oficiais de informações cadastrais. Caso constatada desconformidade, a **CONTRATADA** deverá apresentar os comprovantes ou justificativas para avaliação da **PRODESP**, sob pena de aplicação das sanções previstas neste Contrato.

8.15.3. Havendo a renovação contratual, a **CONTRATADA** deverá reapresentar os documentos de qualificação técnica, inicialmente exigidos e apresentado e que possuem validade vencida ao longo do período, tais como, mas não se limitando a: certificações, registros, inscrição em entidade profissional competente ou alvará/licença/autorização para atuação.

8.16. De forma a garantir o sigilo das informações às quais terá acesso, a **CONTRATADA** deve assinar o Termo de Confidencialidade, Sigilo e Uso – Anexo II.

8.17. A **CONTRATADA** obriga-se a proteger os direitos adquiridos pela **PRODESP**, em razão deste Contrato, das consequências de eventuais questionamentos de terceiros quanto à propriedade autoral e ou industrial brasileira da **CONTRATADA** sobre os programas e manuais, bem como quanto ao direito da **CONTRATADA** de licenciar o uso dos programas e manuais, e obriga-se a defender e indenizar a **PRODESP** de toda e qualquer reclamação decorrente de violação desses direitos, desde que:

8.17.1. A **PRODESP** notifique a **CONTRATADA** por escrito, em até 30 (trinta) dias, do início da ação;

8.17.2. A **CONTRATADA** tenha total controle da defesa e de todas as negociações a ela relacionadas; e

8.17.3. A **PRODESP** forneça à **CONTRATADA** toda assistência, informação e autoridade que se façam necessárias para que a **CONTRATADA** desempenhe as obrigações decorrentes desta cláusula. Cabe à **CONTRATADA** o ressarcimento de despesas incorridas pela **PRODESP** na salvaguarda de seus direitos.

8.17.3.1. Na eventualidade de qualquer programa fornecido pela **CONTRATADA** infringir direitos autorais e/ou industriais, a **CONTRATADA**, de comum acordo com a **PRODESP**, terá a opção de, às suas custas: a) modificar o programa a fim de torná-lo não infrator; b) obter para a **PRODESP** licenças para que este possa continuar o uso dos programas ou manuais ou c) rescindir a licença do programa infrator e reembolsar a **PRODESP** pelo valor correspondente a duas vezes o preço pago, corrigido pela variação do IPC-FIPE – Índice de Preço ao Consumidor, ocorrido no período compreendido entre data base de preço do faturamento até a data da ocorrência. Esta cláusula estabelece a total responsabilidade da **CONTRATADA** e a compensação exclusiva a que a **PRODESP** terá direito pela infração.

8.17.3.2. Qualquer medida judicial que determine que a **PRODESP** deva suspender o uso do programa de computador com fundamento em violação a direitos de terceiros, obrigará a **CONTRATADA**, às suas expensas, providenciar a continuidade de uso com programa de computador similar. Caso não seja possível, a **CONTRATADA** deverá indenizar a **PRODESP** pelo valor correspondente a duas vezes o preço da aquisição do programa de computador, corrigido pela variação do IPC-FIPE ocorrida no período compreendido entre a data base de preço do faturamento até a data da ocorrência. A medida contra ela movida com base nos motivos acima mencionados deve ser objeto de comunicação escrita à **CONTRATADA** a ser instruída com toda a documentação pertinente à ação.

8.17.3.3. A **CONTRATADA** será responsável por danos causados à **PRODESP**, em virtude de produtos e serviços em desconformidade com as garantias definidas neste instrumento, até o limite de duas vezes o preço pago pela **PRODESP**, corrigido pela variação do IPC-FIPE ocorrida no período compreendido entre a data base de preço do faturamento até a data da ocorrência.

8.18. Conhecer e cumprir, naquilo que lhe couber, o Programa de Integridade e o Código de Conduta e Integridade da **PRODESP**, disponíveis no site da **PRODESP** -

endereço eletrônico: Prodesp.sp.gov.br/institucional/código-de-conduta-e-integridade.

8.19. Assinar o "Termo de Ciência e de Notificação", Anexo III deste contrato, dando ciência da remessa da documentação do procedimento ao Tribunal de Contas do Estado de São Paulo.

8.19.1. Providenciar o cadastro de seus representantes legais responsáveis pela assinatura do "Termo de Ciência e de Notificação" no Cadastro Corporativo TCESP – CadTCESP e mantê-lo atualizado, para fins de cadastramento em processo eletrônico, nos termos das Instruções nº 01 de 2024, do Tribunal de Contas do Estado de São Paulo;

8.19.2. Ficará a critério da **CONTRATADA** o acompanhamento do processo junto àquela corte, cabendo-lhe as diligências para juntada da procuração nomeando seus representantes legais/procuradores e demais atos que se fizerem necessários.

8.20. Assinar, ao término da vigência do presente contrato, o Termo de Encerramento e Outras Avenças, conforme modelo Anexo IV deste instrumento.

IX - OBRIGAÇÕES DA PRODESP

9.1. Expedir o(s) Termo(s) de Aceite no prazo estabelecidos na Cláusula III – ACEITE.

9.2. Efetuar os pagamentos no prazo previsto na cláusula VI - FATURAMENTO E PAGAMENTO.

9.3. Comunicar à **CONTRATADA** as ocorrências que demandem assistência técnica, para a adequada abertura de chamada técnica e consequente mobilização do seu pessoal técnico.

9.4. Assinar, ao término da vigência do presente contrato, o Termo de Encerramento e Outras Avenças, conforme modelo Anexo IV deste instrumento.

X – CONFIDENCIALIDADE

10.1. A **CONTRATADA** obriga-se, por seus administradores, sócios e gerentes, por seus funcionários ou terceiros contratados e/ou subcontratados, credenciados e representantes, a manter e guardar o mais expresso, estrito e absoluto sigilo sobre dados, informações, conteúdo, especificações técnicas, características de ambientes, relações ou informações de caráter comercial com clientes da **PRODESP**, a que tenham acesso ou conhecimento, sob qualquer forma, em decorrência da prestação dos serviços e/ou fornecimento de bem, objeto deste contrato, no decorrer da sua execução ou cumprimento, sob pena de responder civil e criminalmente pelo seu descumprimento, ficando responsável pela reparação por prejuízos materiais, morais, perdas e danos e lucros cessantes decorrentes.

10.1.1. O descumprimento das obrigações estabelecidas acima obriga a **CONTRATADA**, a qualquer tempo, ao pagamento, em favor da **PRODESP**, da multa prevista no subitem 14.5.5.

10.1.2. A obrigação de sigilo prevista no item 10.1., aplica-se não só pelo prazo de vigência ou de execução dos serviços/fornecimento previstos neste contrato como se estende também após seu encerramento pelo prazo de 10 (dez) anos.

XI – NORMAS, PARÂMETROS E RESPONSABILIDADES DE PROTEÇÃO DE DADOS

11.1. Os serviços a serem contratados deverão observar as normas técnicas, a legislação aplicável e pertinente à celebração de contratos do Poder Público, bem como as normas e diretrizes à Proteção de Dados, sob pena de aplicação das penalidades constantes da lei e do contrato.

11.2. Como parâmetros mínimos de referência para execução dos serviços, e em observância ao atendimento aos padrões de qualidade, objeto do contrato e dos serviços prestados pela **PRODESP**, deverão ser observadas as seguintes premissas.

11.2.1. Segurança da Informação;

11.2.2. Proteção dos Dados, considerando os fundamentos básicos de respeito à privacidade, autodeterminação informativa, inviolabilidade da intimidade, honra e imagem.

11.3. A **CONTRATADA** se obriga ao cumprimento das seguintes condições e medidas de Segurança da Informação:

11.3.1. Adotar todas as medidas de segurança, sejam elas técnicas e/ou administrativas objetivando a proteção, privacidade e sigilo dos dados e informações à que tiver acesso, durante todo o contrato, bem como durante o ciclo operacional de serviços prestados, desde a coleta, tratamento e descarte dos dados, incluindo o armazenamento, comunicação e sistemas utilizados, acidentais ou ilícitos como destruição, perda, alteração ou qualquer outra forma inadequada ou ilícita;

11.3.2. Comunicar à **PRODESP** qualquer ocorrência e/ou incidente de segurança que possa comprometer ou acarretar risco e, danos aos dados tratados;

11.3.3. Não compartilhar ou comercializar qualquer dado ou informação obtidos em decorrência da prestação de serviços, sem a expressa e formal autorização da **PRODESP**;

11.3.4. Observar e seguir todas as orientações e procedimentos acordados com a **PRODESP**, não realizando nenhum tratamento que não esteja expressa e

previamente autorizado, não coletando nenhum dado ou informação, além do expressamente autorizado;

11.3.5. Ao término do tratamento que envolve a operação de que trata a prestação de serviços contratados, descartar os dados coletados de maneira segura, de sorte a impedir que ocorra sua recuperação;

11.3.6. A **CONTRATADA** deverá disponibilizar evidências técnicas e/ou relatórios de auditoria que comprovem a aplicação das medidas de segurança descritas nesta cláusula, sempre que solicitado pela **PRODESP;**

11.3.7. A **CONTRATADA** assume integral responsabilidade legal, seja civil, penal e/ou administrativa, por eventuais danos materiais e/ou pessoais que forem causados à **PRODESP**, ao Governo do Estado de SÃO PAULO ou a terceiros, caso não seja observada e cumprida qualquer obrigação assumida no Contrato e seus anexos, bem como na legislação brasileira de Proteção de Dados;

11.3.8. A **CONTRATADA** assume, além das responsabilidades previstas no Contrato, o uso responsável das informações a que tiver acesso, zelando pela sua segurança e confidencialidade, de forma a garantir o direito à privacidade de seus proprietários;

11.3.9. O descumprimento às obrigações previstas no Contrato e a infringência a qualquer disposição de Proteção de Dados, implicará na responsabilidade da **CONTRATADA** na assunção das penalidades previstas na legislação vigente.

XII – POLÍTICA ANTICORRUPÇÃO

12.1. As Partes declaram que têm plena ciência das normas de prevenção à corrupção vigentes na legislação brasileira, incluindo, mas não se limitando à Lei Lei nº 8.429/1992 (Lei de Improbidade Administrativa), à Lei nº 12.846/2013, e ao Decreto Estadual nº 67.301/2022, juntamente com seus respectivos regulamentos ("Leis Anticorrupção"). Comprometem-se a observar estritamente tais normas, tanto em seu nome quanto em nome de seus sócios, administradores, colaboradores, e terceiros por elas contratados.

12.2. Ambas as Partes se obrigam a abster-se de dar, oferecer ou prometer, direta ou indiretamente, qualquer bem, valor ou vantagem indevida a agentes públicos, seus relacionados, familiares ou a qualquer pessoa física ou jurídica, com o intuito de obter benefício indevido, influenciar decisões, ou direcionar negócios de forma ilícita;

12.3. Em atendimento à Lei nº 12.846, de 2013, e ao Decreto estadual nº 67.301, de 2022 a **CONTRATADA** se compromete a adotar uma conduta ética e a abster-se de práticas que possam ser caracterizadas como corrupção, suborno, extorsão, pagamento de facilitação, fraude ou quaisquer atos lesivos à administração pública nacional ou estrangeira, ou a terceiros, de modo que a **CONTRATADA** 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.

12.4. A **CONTRATADA** declara que conhece e irá observar as regras e diretrizes estabelecidas no Código de Conduta e Integridade da **PRODESP**, bem como em suas Políticas e Normas a ela aplicáveis.

12.5. A **CONTRATADA** se compromete a informar prontamente a **PRODESP** sobre qualquer processo administrativo ou judicial em que seja envolvida por práticas ilícitas de atos corrupção, lavagem de dinheiro, trabalho escravo, utilização de qualquer trabalho de menor de 16 (dezesseis), anos exceto na condição de aprendiz para os maiores de 14 (quatorze) anos, utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, ou suborno no prazo de 15 (quinze) dias úteis a contar do conhecimento do fato. A falha em informar qualquer uma dessas circunstâncias constituirá justa causa para a resolução imediata do Contrato, conforme previsto nas cláusulas de rescisão e penalidades.

12.6. A **PRODESP** se reserva o direito de realizar auditorias, sempre que julgar necessário, por si ou por terceiros designados, nas atividades da **CONTRATADA** para verificar a conformidade com as legislações anticorrupção e as disposições deste contrato.

12.7. A **CONTRATADA** deverá colaborar integralmente com as auditorias, fornecendo documentos, registros, acesso às instalações e quaisquer outras informações necessárias de maneira oportuna, sob pena de multa compensatória de 5% do valor do contrato, sem prejuízo da indenização suplementar, em caso de obstrução ou não cooperação.

12.8. Caso a **CONTRATADA** venha a ser condenada em decorrência de atos lesivos à administração pública, nos termos da Lei 12.846/2013 ou outra legislação aplicável, deverá ressarcir integralmente a **PRODESP** por todas as multas, indenizações ou quaisquer outros encargos financeiros que esta venha a arcar como consequência dos atos ilícitos praticados pela **CONTRATADA**.

12.9. A **CONTRATADA** deverá indenizar a **PRODESP** por quaisquer outros prejuízos financeiros, diretos ou indiretos, decorrentes da prática desses atos, incluindo, mas não se limitando a perdas reputacionais, custos com defesa jurídica e danos à imagem da **PRODESP**.

12.10. **CONTRATADA** deverá garantir que seus colaboradores e terceiros contratados, especialmente aqueles que atuam diretamente em nome da **PRODESP** ou em situações que envolvam interações com o poder público, participem de programas de treinamento regulares sobre compliance e legislação anticorrupção, garantindo que estejam adequadamente informados sobre as condutas esperadas e as consequências do não cumprimento destas normas. A **PRODESP** poderá, a seu critério, fornecer treinamento adicional para a **CONTRATADA** em relação a seu programa de integridade e compliance.

12.11. O descumprimento de qualquer disposição destas cláusulas constituirá justa causa para a resolução unilateral deste Contrato, a critério da **PRODESP**, sem prejuízo da aplicação de multas contratuais ou da exigência de indenização suplementar por perdas e danos, conforme os artigos 408 e 416 do Código Civil, 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.

XIII - RESPONSABILIDADE E GARANTIA EM SOLUÇÕES COM INTELIGÊNCIA ARTIFICIAL

13.1. Responsabilidade Técnica e Legal da CONTRATADA:

13.1.1. A **CONTRATADA** declara que a solução contratada possui componentes de Inteligência Artificial (IA) embarcados, desenvolvidos em conformidade com os princípios legais, éticos e técnicos aplicáveis, incluindo, mas não se limitando, à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), ao Marco Civil da Internet (Lei nº 12.965/2014). A **CONTRATADA** assume integral responsabilidade por quaisquer falhas, omissões, vícios ocultos, decisões automatizadas indevidas ou danos decorrentes do funcionamento da IA, inclusive aqueles que venham a se manifestar após a entrega da solução.

13.2. Garantia de Conformidade, Disponibilidade e Suporte Técnico:

13.2.1. A **CONTRATADA** compromete-se a prestar garantia integral e disponibilidade da solução pelo prazo vigente do contrato, contados a partir da data de aceite técnico, abrangendo correções de falhas, atualizações de segurança, mitigação de vieses algorítmicos e suporte técnico especializado. A correção de falhas críticas deverá ocorrer no prazo máximo de 04 (quatro) horas (Conforme Tabela NMS – item 2.15.2. deste contrato) após a notificação formal da **PRODESP**.

13.3. Transparência e Explicabilidade:

13.3.1. A **CONTRATADA** garante que os modelos de IA embarcados na solução possuem mecanismos de auditabilidade, rastreabilidade e explicabilidade, permitindo a **PRODESP** compreender os critérios utilizados nas decisões automatizadas, bem como contestá-las, quando necessário.

13.4. Mitigação de Riscos e Supervisão Humana:

13.4.1. A solução deverá conter salvaguardas técnicas que permitam supervisão humana sobre decisões automatizadas, especialmente aquelas que possam impactar direitos fundamentais, operações críticas ou relações contratuais. A **CONTRATADA** deverá implementar mecanismos de controle que permitam a **PRODESP** intervir ou desativar funcionalidades da IA em caso de risco iminente ou comportamento indevido.

13.5. Continuidade Operacional e Portabilidade:

13.5.1. Em caso de rescisão contratual, a **CONTRATADA** deverá assegurar a continuidade operacional da solução por um período de transição de 30 (trinta) dias, bem como a portabilidade dos dados e configurações técnicas, em formato interoperável, sem ônus adicional a **PRODESP**.

XIV - RESCISÃO E PENALIDADES

14.1. O contrato poderá ser rescindido na forma, com as consequências e pelos motivos previstos no artigo 81 do Regulamento Interno de Licitações e Contratos da **PRODESP**, sujeitando-se a **CONTRATADA** às penalidades previstas neste contrato.

14.2. No caso de a **CONTRATADA** estar em situação de recuperação judicial, a convalidação em falência ensejará a imediata rescisão deste contrato, sem prejuízo da aplicação das demais cominações legais.

14.3. O presente contrato poderá ser rescindido por qualquer das partes, pelo não cumprimento de qualquer condição ou cláusula estabelecida neste instrumento, ficando a parte infratora sujeita, a favor da parte inocente, às perdas e danos correspondentes.

14.4. Os casos fortuitos e/ou motivos de força maior serão excludentes da responsabilidade das partes contratantes de acordo com o disposto no artigo 393 do Código Civil Brasileiro.

14.5. Pela inexecução total ou parcial de qualquer cláusula e/ou condição do contrato a **PRODESP** poderá, garantida a prévia defesa, aplicar à **CONTRATADA** as seguintes sanções:

14.5.1. Advertência;

14.5.2. Multa equivalente a 10% (dez por cento) calculada sobre o valor total do contrato, no caso de rescisão, por culpa ou requerimento da **CONTRATADA**, sem motivo justificado ou amparo legal, a critério da **PRODESP**.

14.5.3. No caso de descumprimento dos Níveis Mínimos de Serviço, previsto no item 2.15. deste contrato, serão aplicadas as penalidades estabelecidas na tabela do subitem 2.15.2. deste instrumento.

14.5.4. Multa equivalente a 5% (cinco por cento) calculada sobre o valor do faturamento do mês da ocorrência, por infringência de qualquer cláusula, condições ou obrigações pactuadas neste contrato e não abrangidas pelas alíneas anteriores. Não havendo faturamento no mês da ocorrência, a multa será de 0,4% (zero vírgula quatro por cento) calculada sobre o valor total do contrato.

14.5.4.1. Em caso de reincidência do descumprimento contratual, a multa estabelecida terá seu percentual acrescido em 50% (cinquenta por cento).

14.5.5. Multa de 20% (vinte por cento) do valor total do contrato, devidamente corrigido pelo IPC-FIPE, para o descumprimento do estipulado na cláusula X - CONFIDENCIALIDADE deste contrato, sem prejuízo da cobrança de todos os prejuízos materiais e morais, custas, despesas processuais, honorários advocatícios, correção monetária e demais cominações processuais e legais, pelo ajuizamento da competente ação judicial de perdas e danos contra a **CONTRATADA**;

14.5.6. Suspensão temporária de participação em licitação e impedimento de contratar com a **PRODESP**, por prazo não superior a 2 (dois) anos.

14.6. Ficará a critério da **PRODESP** a aplicação cumulativa ou não das penalidades acima.

14.7. As multas previstas neste contrato poderão ser descontadas dos pagamentos devidos ou cobrados da **CONTRATADA** através de cobrança direta e autônoma, pela via administrativa ou judicial.

14.8. As penalidades serão aplicadas sem prejuízo das multas previstas no ato convocatório, após ter sido garantido o exercício do direito de defesa e registradas na plataforma e-Sanções da Bolsa Eletrônica de Compras-BEC.

14.9. No caso de não existirem pagamentos pendentes, a **CONTRATADA** deverá efetuar a quitação da multa em até 48 (quarenta e oito) horas contadas do recebimento do documento de cobrança respectivo, por meio de depósito bancário, sob pena de, em não o fazendo, sujeitar-se aos procedimentos judiciais cabíveis.

14.10. Os valores referentes às multas, indenizações e demais importâncias quando não ressarcidos pela **CONTRATADA**, serão atualizados pelo IPC-FIPE, calculado *pro rata dia* e acrescido de juros de mora de 12% (doze por cento), ao ano.

14.11. Sem prejuízo da aplicação de penalidades, a **CONTRATADA** é responsável pelos danos causados à **PRODESP** ou a terceiros, na forma disposta no artigo 76 da Lei federal nº 13.303/2016, não excluindo ou reduzindo essa responsabilidade, a fiscalização ou acompanhamento pelo órgão interessado.

14.12. As partes poderão rescindir o presente contrato, mediante acordo.

XV - DISPOSIÇÕES FINAIS

15.1. O presente contrato é regido pelas suas cláusulas, pelo disposto na Lei Federal nº 13.303/2016 e pelo Regulamento Interno de Licitações e Contratos da **PRODESP**, além dos preceitos de direito privado, pelas Leis Federais nº 9.609 (Lei do Software) e 9.610 (Lei de Direitos Autorais) de 19/02/1998 e demais normas regulamentares aplicáveis à espécie.

15.2. O presente contrato, a execução de seu objeto, produtos e/ou serviços não poderão ser cedidos ou transferidos total ou parcialmente, pela **CONTRATADA**, a terceiros estranhos a esta contratação.

15.3. A **PRODESP** poderá, sem a necessidade de anuência da **CONTRATADA**, utilizar os produtos e/ou serviços adquiridos por meio deste contrato para a prestação de serviços a seus **CLIENTES** (órgãos ou entidades públicas da Administração Direta e Indireta, vinculados aos Governos Estadual e Municipais no Estado de São Paulo).

15.4. O cumprimento, durante a execução dos serviços, das leis federais, estaduais e municipais vigentes, correrá por conta da **CONTRATADA**, sendo a única e exclusiva responsável pelas infrações que houver.

15.5. A **CONTRATADA**, mediante acordo, poderá anuir na cessão ou transferência total ou parcial deste contrato da **PRODESP** para qualquer de seus clientes e/ou entes em geral, mantidas as condições nele estabelecidas.

15.6. Qualquer omissão ou tolerância das partes no exigir o estrito cumprimento das cláusulas e condições deste contrato ou exercer uma prerrogativa dele decorrente, não constituirá renúncia e nem afetará o direito da parte contratante em exercê-lo a qualquer tempo.

15.7. As cláusulas deste contrato prevalecerão sempre em relação a qualquer acordo verbal ou escrito ajustado anteriormente ou posteriormente à data de sua assinatura, exceto se devidamente demonstrado a divergência entre a vontade das partes e o registrado no contrato, ocasião que se providenciará o devido aditamento para retificação do contrato.

15.8. A **CONTRATADA** ficará sujeita à instauração de processo administrativo de responsabilização, sem prejuízo das sanções administrativas previstas nos artigos 83 e 84 da Lei federal nº 13.303/2016, caso incorra na prática de atos que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou que de qualquer forma venham a constituir fraude ou corrupção ao longo da execução deste contrato.

15.9. O disposto neste contrato não poderá ser alterado ou emendado pelas partes, a não ser por meio de Termo Aditivo.

XVI – ANEXOS

16.1. Integram o presente contrato os seguintes anexos:

Anexo I - Termo de Referência;
Anexo II - Termo de Confidencialidade, Sigilo e Uso;
Anexo III - Termo de Ciência e de Notificação – Tribunal de Contas do Estado de São Paulo;
Anexo IV - Termo de Encerramento e Outras Avenças – Modelo.

XVII – FORO

17.1. As partes elegem o foro da comarca de Taboão da Serra, Estado de São Paulo, como único competente para conhecer e dirimir quaisquer questões oriundas do presente contrato, com expressa renúncia de qualquer outro foro, por mais privilegiado que seja.

E, por estarem assim, justas e acertadas, as Partes assinam o presente instrumento.

Taboão da Serra, a data de assinatura deste instrumento corresponde à data da última assinatura digital do(s) representante(s) legal(is).

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

Nome:
Cargo:
CPF:

Nome:
Cargo:
CPF:

CONTRATADA.

Nome:
Cargo:
CPF:

Nome:
Cargo:
CPF:

ANEXO I

TERMO DE REFERÊNCIA

(Anexo I do Edital – Documento SEI n.º _____)

ANEXO II

TERMO DE CONFIDENCIALIDADE, SIGILO E USO

A Contratada **.....**, inscrita no CNPJ sob o número ....., com sede na cidade ....., doravante designada Signatária, neste ato representada por **.....**, inscrito(a) no CPF sob o número ....., aceita as regras, condições e obrigações constantes do presente Termo.

1. O objetivo deste Termo de Confidencialidade, Sigilo e Uso é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva e/ou sob controle do Contratante reveladas ao Signatário ou por ele acessadas em função da execução do objeto do contrato PRO.00.....
2. A expressão “informações restritas” abrange toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: dados pessoais, técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, marcas e modelos utilizados, preços e custos, definições e informações mercadológicas, invenções e ideias, vulnerabilidades existentes, outras informações técnicas, financeiras ou comerciais, entre outros.
3. A Signatária compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do Contratante, das informações restritas reveladas ou acessadas.
4. A Signatária compromete-se a não utilizar, de forma diversa da prevista no contrato celebrado com o Contratante, as informações restritas reveladas ou acessadas.
5. A Signatária deverá cuidar para que as informações reveladas ou acessadas fiquem limitadas ao conhecimento próprio.
6. A Signatária obriga-se a informar imediatamente ao Contratante qualquer violação das regras de confidencialidade, sigilo e uso estabelecidas neste Termo de que tenha tomado conhecimento ou que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.
7. A quebra da confidencialidade, do sigilo ou das condições de uso das informações restritas reveladas ou acessadas, por ação ou omissão do Signatário, devidamente comprovada, sem autorização expressa do Contratante, sujeitará a Signatária às consequências legais e sanções cabíveis, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo Contratante, inclusive os de ordem moral, bem como às responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.
8. O presente Termo tem natureza irrevogável e irretratável.
9. A Signatária manifesta explícita ciência e se compromete a observar as cláusulas de segurança, privacidade e proteção de dados do Contratante, prevista no Contrato PRO.00..... e seus anexos.

E, por aceitar todas as condições e as obrigações constantes do presente Termo, a Signatária assina o presente Termo.

Taboão da Serra, a data de assinatura deste instrumento corresponde a data da última assinatura digital do(s) representante(s) legal(is).

CONTRATADA

Nome:
Cargo:
CPF:

ANEXO III

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO (Contratos)

Contratante: Companhia de Processamento de Dados do Estado de São Paulo – PRODESP

Contratada:

Contrato n° PRO.00.MINUTA

Objeto: Contratação de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação e controles de privacidade de dados.

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial Eletrônico do Tribunal de Contas do Estado de São Paulo (https://doe.tce.sp.gov.br/), em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais dos responsáveis pela contratante estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no Artigo 2º das Instruções nº 01/2024, conforme "Declaração(ões) de Atualização Cadastral" anexa (s);

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:

a) o acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

Taboão da Serra, a data de assinatura deste instrumento corresponde à data da última assinatura digital do(s) representante(s) legal(is).

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome:
Cargo:
CPF:

RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME:

Nome:
Cargo:
CPF:

Nome:
Cargo:
CPF:

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:

Pela CONTRATANTE: Companhia de Processamento de Dados do Estado de São Paulo – PRODESP

Nome:
Cargo:
CPF:

Nome:
Cargo:
CPF:

Pela CONTRATADA:

Nome:
Cargo:
CPF:

Nome:
Cargo:
CPF:

ORDENADOR DE DESPESAS DA CONTRATANTE:

Nome:
Cargo:
CPF:

GESTOR DO CONTRATO:

Nome:
Cargo:
CPF:

FISCALDO CONTRATO:

Nome:
Cargo:
CPF:

Nota: Modelo publicado no Diário Oficial Eletrônico do Tribunal de Contas do Estado de São Paulo, em 24/05/2024

ANEXO IV

TERMO DE ENCERRAMENTO E OUTRAS AVENÇAS DO CONTRATO DE SOLUÇÃO DE PLATAFORMA PARA SEGURANÇA CIBERNÉTICA QUE REALIZA AVALIAÇÃO DO NÍVEL DE RISCO CORPORATIVO E TECNOLÓGICO COM MONITORAMENTO DE MATURIDADE E AUDITORIA, GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E CONTROLES DE PRIVACIDADE DE DADOS, FIRMADO ENTRE A COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP E A _____.

PRO.00.MINUTA

Pelo presente termo, de um lado a **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**, com sede no Município de Taboão da Serra, Estado de São Paulo, na Rua Agueda Gonçalves n.º 240, inscrita no CNPJ/MF sob n.º 62.577.929/0001-35, doravante denominada simplesmente **PRODESP**, e de outro lado, a **_____.**, com sede na _____ - CEP _____, inscrita no CNPJ/MF sob nº _____, doravante designada simplesmente **CONTRATADA**, representadas neste ato por seus representantes legais ao final designados e assinados, resolvem encerrar o contrato de solução de plataforma para segurança cibernética que realiza avaliação do nível de risco corporativo e tecnológico com monitoramento de maturidade e auditoria, governança de segurança da informação e controles de privacidade de dados, mediante a seguinte cláusula e condições:

I – ENCERRAMENTO E OUTRAS AVENÇAS

1.1. As partes, de comum acordo, consideram concluído o objeto do contrato PRO.00.MINUTA em ___ de _____ de 20__, permanecendo as obrigações eventualmente remanescentes, considerando o Termo de Recebimento Definitivo emitido em __/__/20__.

1.2. Em decorrência do encerramento do contrato mencionado no item 1.1. acima, as partes dão-se plena, rasa, mútua, recíproca, irrestrita, irrevogável e irretratável quitação dos serviços e valores referentes ao objeto do contrato PRO.00.MINUTA, para nada mais reclamar a qualquer título.

E, por estarem assim, justas e acordadas, as Partes firmam o presente instrumento.

Taboão da Serra, a data de assinatura deste instrumento corresponde à data da última assinatura digital do(s) representante(s) legal(is).

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

Nome:
Cargo:
CPF:

Nome:
Cargo:
CPF:

CONTRATADA

Nome:
Cargo:
CPF:

ANEXO X

REGULAMENTO INTERNO DE LICITAÇÕES E CONTRATOS DA PRODESP

https://www.prodesp.sp.gov.br/wp-content/uploads/2024/12/Regulamento-Interno-de-Licitacoes-e-Contratos-Prodesp_RILC.pdf