Governo do Estado de São Paulo
Secretaria de Gestão e Governo Digital
Divisão de Contratos

TERMO

Secretaria de Gestão e Governo Digital
Processo Administrativo n.° 018.00001935/2025-17
CONTRATO Nº 084/2025

CONTRATO ADMINISTRATIVO N.º 084/2025 DE PRESTAÇÃO DE SERVIÇOS DE INFORMÁTICA QUE ENTRE SI CELEBRAM, DE UM LADO O ESTADO DE SÃO PAULO, POR MEIO DA **SECRETARIA DE GESTÃO E GOVERNO DIGITAL - SGGD** E DE OUTRO A **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP**.

O ESTADO DE SÃO PAULO , por intermédio da **SECRETARIA DE GESTÃO E GOVERNO DIGITAL,** inscrita no CNPJ/MF sob nº 39.467.292/0017-70, com sede no Município de São Paulo, Estado de São Paulo, na Avenida Rangel Pestana, 300 – 14º e 16º andares - CEP 01017-911, neste ato representado pela Senhora, **OTILIA CARLA DOS SANTOS**, Chefe de Assessoria da **UNIDADE DE GESTÃO DO PROJETO MAIS DIGITAL (UGP)** , nomeada em 05 de agosto de 2025, pela Resolução do Secretario Executivo, publicada no DOE de 06 de agosto de 2025, inscrita no CPF 293.377.078-45, doravante designada simplesmente CONTRATANTE, e **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO - PRODESP** , inscrita no CNPJ/MF sob o nº 62.577.929/0001-35, sediada na Rua Agueda Gonçalves, n.º 240 - Jd. Pedro Gonçalves - Taboão da Serra/SP, doravante designada CONTRATADA, neste ato representada por **THIAGO WALTZ ALVES,** Diretor de Relacionamento com Clientes, inscrito no CPF sob o nº 950.082.761-15 e pelo Senhor **GILENO GURJÃO BARRETO**, Diretor-Presidente, inscrito no CPF sob o nº 315.099.595-72, conforme atos constitutivos da fornecedora, tendo em vista o que consta no Processo nº 018.00020025/2024-52 e em observância às disposições constantes no Contrato de Empréstimo BID 5579/OC-BR (BR-L1591), amparado no art. 1º, §3º, II, da Lei 14.133/21, e aplicação das normas de contratação previstas nas Políticas de Aquisições do BID, reunidas no documento GN-2349-15 e demais normas da legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente da Contratação Direta, mediante as condições a seguir enunciadas, de acordo com as subdivisões subsequentes na forma de cláusulas e respectivos itens que compõem este instrumento.

1. CLÁUSULA PRIMEIRA - OBJETO

1.1 O objeto do presente instrumento é a contratação de serviços especializados para a operação de um Centro de Operações de Segurança (Security Operations Center – SOC) no modelo de serviço gerenciado. O foco inicial é o monitoramento contínuo, a gestão de vulnerabilidades, a detecção, análise, resposta e o reporte de incidentes de segurança da informação. Essa iniciativa busca garantir a proteção dos ativos, a mitigação de riscos cibernéticos, o atendimento às normas aplicáveis e boas práticas, além de promover o aumento da maturidade em segurança cibernética.

1.2 O preço para execução dos serviços constantes desta ESP é estimado em **R$ 62.652.009,24 (sessenta e dois milhões, seiscentos e cinquenta e dois mil nove reais e vinte e quatro centavos)**, tendo como data base de referência o mês de outubro/2025 e será reajustado de acordo com as condições estabelecidas no contrato a que se vincula.

ITEM	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	QTDE PREVISTA		VALOR UNITÁRIO	QTDE MESES	VALOR PREVISTO	
			QTDE MÊS	QTDE TOTAL			PARCELA MENSAL	TOTAL
5.1	**Paas Middleware**						**R$ 4.784.065,32**	**R$ 57.408.783,84**
5.1.1	Pass Middleware	UNIDADE DE MIDDLEWARE / MÊS	2829	33948	R$ 1.691,08	12	R$ 4.784.065,32	R$ 57.408.783,84
5.2	**Gestão**						**R$ 436.935,45**	**R$ 5.243.225,40**
5.2.1	Serviço de Gestão de Operações Prata	POR UNIDADE DE GESTÃO / MÊS	1	12	R$ 84.733,05	12	R$ 84.733,05	R$ 1.016.796,60
5.2.2	Serviço de Gestão de Operações Ouro	POR UNIDADE DE GESTÃO / MÊS	2	24	R$ 176.101,20	12	R$ 352.202,40	R$ 4.226.428,80
TOTAL							**R$ 5.221.000,77**	**R$ 62.652.009,24**

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

1.3.1 O Termo de Referência;

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

1.3.3. A Proposta do Contratado consubstanciada nas Especificação de Serviços e Preços" **E0250354**;

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

1.3.5. Política do Banco sobre Práticas Proibidas ;

1.3.6. Demais anexos dos documentos supracitados.

1.4 Na execução e interpretação do contrato, deverão ser observadas as normas do BID, quando houver regulamentação específica quanto ao assunto, cabendo a aplicação subsidiária da Lei 14.133/2021 nos demais pontos em que o regulamento BID não delimitar os parâmetros ou não regular a matéria.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1 O prazo de vigência da contratação é de 12 (doze) meses, contados da data de sua assinatura, podendo ser prorrogado de acordo com os termos previstos nas Políticas de Aquisições do BID, durante a vigência do Contrato de Empréstimo nº 5579/OC-BR, observadas, no que couber, as disposições dos artigos 106 e 107 da Lei n° 14.133, de 2021.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

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

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

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

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

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

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

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

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor estimado do presente contrato é de **R$ 62.652.009,24** (sessenta e dois milhões, seiscentos e cinquenta e dois mil nove reais e vinte e quatro centavos), mês de referência outubro/2025, sendo **R$ 2.610.500,39** (dois milhões, seiscentos e dez mil e quinhentos reais e trinta e nove centavos) **para o exercício de 2025**, **R$60.041.508,80** (sessenta milhões, quarenta e um mil quinhentos e oito reais e oitenta centavos) **para o exercício de 2026**, com recursos financeiros oriundos do Contrato de Empréstimo nº 5579/OC-BR e do Tesouro, na dotação orçamentária a seguir: Fonte 175.478.090 e 150.010.001, respectivamente; Natureza de Despesa 33904090, PTRES 530157 e Programa de Trabalho 04.126.5302.2656.

5.2. No valor acima estão incluídas todas as despesas diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação. O valor indicado nesta cláusula é meramente estimativo, de forma que os pagamentos devidos ao Contratado dependerão dos quantitativos efetivamente demandados, medidos e fornecidos.

6. CLÁUSULA SEXTA - RECEBIMENTO E PAGAMENTO

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

6.2. Da Execução dos Serviços e das Condições para Faturamento

a) Execução condicionada à emissão de Ordem de Serviço (OS)

a.1) A execução de quaisquer serviços objeto deste contrato somente poderá ocorrer mediante emissão prévia de Ordem de Serviço – OS, formalmente expedida e autorizada pela gestão contratual. É expressamente vedado o início de qualquer atividade sem a correspondente OS, que estabelecerá, de maneira detalhada, o escopo, as entregas, os prazos, os responsáveis, as condições de execução e demais parâmetros necessários ao adequado acompanhamento e controle.

a.2) A emissão da OS está condicionada à observância das prioridades estratégicas definidas pela Administração e à comprovação de disponibilidade orçamentária para o exercício, constituindo requisito indispensável para a validade e regularidade da execução contratual.

b) Medição obrigatória das entregas

Cada entrega realizada pela contratada será submetida à medição formal, nos termos estabelecidos pela Administração, constituindo condição indispensável para fins de faturamento. O pagamento somente incidirá sobre os serviços efetivamente prestados, conferidos e aceitos pela gestão e fiscalização contratual, vedado qualquer faturamento que exceda os quantitativos, escopos e limites previstos neste contrato.

6.3. O pagamento será efetuado através do Sistema de Administração Financeira de Estados e Municípios – SIAFEM, na Unidade Gestora 533284/53091, Conta Única, no prazo de 30 (trinta) dias (Decreto nº 43.914, de 26/03/99), contados da data de entrega da nota fiscal/fatura dos serviços prestados diretamente pela PRODESP.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.16 O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

6.16.1 Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, a contar de seu recebimento pela Administração, na forma desta seção, prorrogáveis por igual período, justificadamente, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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

6.17.1 o prazo de validade;

6.17.2 a data da emissão;

6.17.3 os dados do contrato e do órgão contratante;

6.17.4 o período respectivo de execução do contrato;

6.17.5 o valor a pagar; e

6.17.6 eventual destaque do valor de retenções tributárias cabíveis.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. CLÁUSULA SÉTIMA - REAJUSTE

7.1 Os preços inicialmente ajustados são fixos e irreajustáveis pelo prazo de 12 (doze) meses.

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

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1 São obrigações do Contratante:

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

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

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

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

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

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

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

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

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

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

8.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo Contratado no prazo máximo de 60 (sessenta) dias, contado a partir da conclusão da instrução do requerimento, sendo admitida a prorrogação motivada desse prazo por igual período, e observado o disposto no parágrafo único do artigo 131 da Lei nº 14.133, de 2021.

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

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9.1.21.1. De igual modo, a cessão à Administração Contratante abrange os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, códigos-fonte de aplicações, modelos de dados e as bases de dados respectivas;

9.1.21.2. A cessão de direitos de propriedade intelectual não abrange direitos da CONTRATADA pré-existente à celebração deste contrato, nem direitos de propriedade intelectual pertencentes a terceiros eventualmente licenciados à PRODESP.

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

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

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

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

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

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

10. CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

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

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

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

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

10.1.4. O Contratado deve:

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

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

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

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

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

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

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

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

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

10.1.12. Eventual transferência de dados pessoais para fora do território nacional somente poderá ocorrer mediante comunicação ao CONTRATANTE, devendo o CONTRATADO demonstrar, previamente, a observância das salvaguardas e condições previstas na Lei Federal nº 13.709/2018 e na Resolução CD/ANPD nº 19, de 23 de agosto de 2024.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1 Não haverá exigência de garantia contratual da execução.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1 Comete infração administrativa, o Contratado que:

a) der causa à inexecução parcial do contrato;

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

c) der causa à inexecução total do contrato;

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

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

f) praticar ato fraudulento na execução do contrato;

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

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

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

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

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

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

iv) Multa:

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

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

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

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

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

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

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

(7) Para a infração descrita na alínea “a” do item 12.1, a multa será 0,5% (cinco décimos por cento) a 30% (trinta por cento) do valor do Contrato, ressalvadas as seguintes infrações:

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

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

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

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

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

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

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

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

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

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

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

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

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

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

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

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

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

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

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

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

13.3.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.3.2 Relação dos pagamentos já efetuados e ainda devidos;

13.3.3 Indenizações e multas.

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

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

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

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

I. Fonte 175478090 e 150010001;

II. Natureza de Despesa 33904090;

III. PTRES 530157;

IV. Programa de Trabalho 04.126.5302.2656.

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

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1 Aplicam-se as Políticas de Aquisições do BID e, nos cados omissos, serão aplicadas disposições contidas na Lei n.º 14.133, de 2021, e disposições regulamentares pertinentes, e, subsidiariamente, as disposições contidas na Lei n.º 8.078, de 1990 - Código de Defesa do Consumidor - e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

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

16.2 O Contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários no objeto, a critério exclusivo do Contratante, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3 Se o contrato não contemplar preços unitários para serviços cujo aditamento se fizer necessário, esses serão fixados por meio da aplicação da relação geral entre os valores da proposta e o do orçamento-base da Administração sobre os preços referenciais ou de

mercado vigentes na data do aditamento, respeitados os limites estabelecidos no artigo 125 da Lei nº 14.133, de 2021.

16.4 Eventuais alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, respeitadas as disposições da Lei nº 14.133, de 2021, admitindo-se que, nos casos de justificada necessidade de antecipação de seus efeitos, a formalização do aditivo ocorra no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.5 Caso haja alteração unilateral do contrato que aumente ou diminua os encargos do Contratado, o equilíbrio econômico-financeiro inicial será restabelecido no mesmo termo aditivo.

16.6. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

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

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

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

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

18. CLÁUSULA DÉCIMA OITAVA– FORO

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

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

assinado digitalmente
OTILIA CARLA DOS SANTOS
Unidade de Gestão do Projeto São Paulo Mais Digital
Secretaria de Gestão e Governo Digital

assinado digitalmente
THIAGO WALTZ ALVES
Diretor de Relacionamento com Clientes
Companhia de Processamento de Dados do Estado de São Paulo PRODESP

assinado digitalmente
GILENO GURJÃO BARRETO
Diretor-Presidente
Companhia de Processamento de Dados do Estado de São Paulo PRODESP

ANEXO I

TERMO DE REFERÊNCIA

1. CONTEXTUALIZAÇÃO E COMPONENTE

A crescente digitalização dos serviços públicos e a interconexão dos sistemas governamentais têm ampliado exponencialmente a superfície de exposição a riscos cibernéticos no âmbito da Administração Pública. No Estado de São Paulo, essa realidade impõe a necessidade de uma abordagem estruturada, preventiva e contínua de proteção aos ativos de informação e à infraestrutura crítica dos órgãos estaduais.

Em um cenário de ameaças cada vez mais sofisticadas e persistentes, a inexistência de mecanismos centralizados de monitoramento e resposta fragiliza a capacidade institucional de prevenir, detectar e mitigar incidentes cibernéticos em tempo hábil, colocando em risco a continuidade dos serviços públicos essenciais e a integridade de dados sensíveis sob a custódia do Estado.

Nesse contexto, a implantação de um Centro de Operações de Segurança (*Security Operations Center* – SOC) surge como medida estratégica e urgente. O SOC permitirá o acompanhamento ininterrupto de eventos de segurança (24x7), com capacidade de triagem, análise, correlação de alertas, resposta técnica a incidentes e acionamento célere das equipes especializadas da Secretaria de Gestão e Governo Digital (SGGD). Trata-se de uma infraestrutura fundamental para garantir a resiliência dos serviços digitais, elevar o nível de maturidade cibernética da Administração Pública.

Estudos recentes reforçam a urgência de fortalecer a segurança cibernética na administração pública. O relatório "2024 *Data Breach Investigations Report*" da Verizon analisou mais de 30 mil incidentes de segurança e identificou que 68% das violações envolveram o elemento humano, incluindo erros e engenharia social. Além disso, 32% das violações utilizaram técnicas de extorsão, como *ransomware*, e 15% envolveram terceiros, destacando riscos na cadeia de suprimentos. A exploração de vulnerabilidades como ponto de entrada inicial para violações cresceu 180% em relação ao ano anterior (DIRB, 2024, disponível em: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf).

Complementarmente, as tendências de cibersegurança para 2025, conforme identificado pela Gartner, destacam a necessidade de programas de cibersegurança mais focados que enfatizem a continuidade dos negócios e a gestão colaborativa de riscos. Isso inclui a adoção crescente de IA generativa, a contínua migração para a nuvem e o aumento das obrigações regulatórias, exigindo uma abordagem mais resiliente e adaptativa na gestão da segurança da informação (Gartner, 2025, disponível em: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends).

A contratação do SOC no âmbito do Projeto São Paulo Mais Digital, financiado com recursos do Banco Interamericano de Desenvolvimento (BID), representa uma resposta concreta a esse cenário. Buscando consolidar uma estrutura de defesa cibernética moderna, interoperável e aderente às melhores práticas, alinhando-se aos princípios definidos pela Estratégia de Governo Digital do Estado de São Paulo e às competências atribuídas à SGGD quanto à segurança cibernética. A contratação insere-se no Componente 2 – Infraestrutura de TIC e Conectividade do Projeto São Paulo Mais Digital, com foco no aprimoramento das capacidades de proteção cibernética do Estado.

CONTRATAÇÃO DE SERVIÇO DE SECURITY OPERATION CENTER (SOC) – FASE INICIAL CONTEMPLANDO O MONITORAMENTO DE INCIDENTES CIBERNÉTICOS

2. OBJETO DA CONTRATAÇÃO

O Termo de Referência tem como objetivo a contratação de serviços especializados para a operação de um Centro de Operações de Segurança (Security Operations Center – SOC) no modelo de serviço gerenciado. O foco inicial é o monitoramento contínuo, a gestão de vulnerabilidades, a detecção, análise, resposta e o reporte de incidentes de segurança da informação. Essa iniciativa busca garantir a proteção dos ativos, a mitigação de riscos cibernéticos, o atendimento às normas aplicáveis e boas práticas, além de promover o aumento da maturidade em segurança cibernética.

3. ÓRGÃOS PARTICIPANTES

A contratação abrangerá a SGGD e outros órgãos que venham a ser definidos como estratégicos ou que apresentem menor grau de maturidade em Segurança Cibernética, conforme diagnóstico a ser conduzido pela Subsecretaria de Governo Digital (SGD). Essa abordagem permitirá a concentração de esforços na construção de uma base sólida e escalável em segurança cibernética, garantindo que os objetivos estabelecidos sejam alcançados de forma eficiente e alinhada com as expectativas.

4. JUSTIFICATIVA DA CONTRATAÇÃO

A Secretaria de Gestão e Governo Digital do Estado de São Paulo (SGGD), conforme o Decreto nº 69.052, de 14 de novembro de 2024, é responsável pela coordenação da implementação de políticas de cibersegurança na Administração Pública estadual. Em observância ao Decreto nº 67.435, de 1º de janeiro de 2023, compete à SGGD a formulação e implementação de diretrizes, normas e padrões técnicos em segurança da informação, bem como a condução de ações de prevenção, detecção, resposta e recuperação diante de incidentes cibernéticos. O Decreto nº 67.799, de 13 de julho de 2023, que institui a Estratégia de Governo Digital do Estado de São Paulo, estabelece como diretriz o fortalecimento da resiliência cibernética da Administração Pública, reconhecendo a segurança como um dos pilares para a transformação digital dos serviços públicos.

A crescente digitalização dos serviços públicos e a expansão do governo digital têm ampliado a superfície de ataque e os riscos cibernéticos para a infraestrutura tecnológica do Estado, tornando a proteção dos ativos de informação uma necessidade crítica. Nesse contexto, a ausência de mecanismos centralizados de monitoramento, detecção e resposta a incidentes compromete a continuidade dos serviços públicos essenciais e a proteção das informações sensíveis sob a guarda do Estado.

A contratação do SOC configura-se como medida essencial para garantir a integridade, disponibilidade e confiabilidade dos ativos de informação da Administração Pública. Essa estrutura viabiliza a detecção proativa de ameaças, a resposta tempestiva a incidentes e a implementação prática de diretrizes estabelecidas por frameworks amplamente reconhecidos. A implantação do SOC permitirá a identificação célere de violações de dados pessoais, com o objetivo de minimizar os impactos decorrentes de incidentes de segurança da informação, assegurando a comunicação tempestiva às autoridades competentes, em observância ao marco legal vigente.

ITEM 4.1 Pilares e Estratégias de Atuação do SOC

O SOC fundamenta-se em pilares e estratégias de atuação voltadas à prevenção e remediação de incidentes, organizadas em disciplinas reconhecidas pelo mercado de segurança da informação, ilustrados na imagem abaixo:

A abordagem do SOC é um modelo estruturado que contempla de forma integrada as funções de monitoramento, prevenção, detecção e remediação. A atuação sinérgica desses pilares viabiliza uma resposta coordenada, eficaz e continuamente adaptável às ameaças cibernéticas. Os três principais pilares que compõem o SOC são:

NOC (Network Operations Center): Embora o SOC seja focado em segurança, a integração com as práticas de um NOC é crucial em ambientes governamentais, onde a disponibilidade de serviços públicos é crítica. O NOC baseia-se no monitoramento e gerenciamento da disponibilidade e desempenho da infraestrutura de rede e sistemas, permitindo uma visão holística e facilitando a distinção entre falhas operacionais e incidentes de segurança. Suas responsabilidades incluem:

· Monitoramento contínuo da disponibilidade de serviços e sistemas críticos;

· Detecção de anomalias de desempenho que podem indicar incidentes de segurança;

· Correlação entre eventos operacionais e de segurança para identificação de ataques complexos;

· Resposta coordenada a incidentes que afetam tanto a segurança quanto a disponibilidade.

CSIRT (Computer Security Incident Response Team): Representa a equipe especializada em resposta a incidentes de segurança, atuando como nível avançado de análise e contenção. No contexto governamental, o CSIRT desempenha papel crucial na resposta a incidentes que podem afetar infraestruturas críticas e serviços essenciais, garantindo recuperação rápida e minimização de impactos. Suas responsabilidades incluem:

· Contenção avançada e erradicação de ameaças persistentes;

· Análise de causa-raiz para identificação de vetores de ataque e falhas de controle;

· Coordenação de resposta a incidentes críticos envolvendo múltiplas equipes e *stakeholders*;

· Desenvolvimento de lições aprendidas e recomendações para prevenção de recorrências.

CTI (Cyber Threat Intelligence): Concentra-se na coleta, análise e disseminação de informações sobre ameaças, permitindo decisões baseadas em inteligência acionável. Para órgãos governamentais, a CTI é essencial para antecipar ameaças direcionadas, incluindo ataques patrocinados por estados- nação e grupos de ameaças avançadas que frequentemente visam infraestruturas governamentais. Abrange:

· Coleta de dados de múltiplas fontes, incluindo *feeds* de inteligência, *deep/dark web* e OSINT (*Open Source Intelligence*);

· Análise contextual de ameaças relevantes para o setor governamental;

· Identificação de TTPs (Táticas, Técnicas e Procedimentos) utilizados por atores maliciosos;

· Produção de inteligência acionável para equipes de segurança e tomadores de decisão;

· Monitoramento proativo de campanhas direcionadas ao setor público.

5. MARCO NORMATIVO

O Termo de Referência encontra amparo nos seguintes instrumentos normativos e de orientação técnica:

· Decreto nº 67.799, de 13 de julho de 2023, que institui a Estratégia de Governo Digital do Estado de São Paulo, estabelecendo como diretrizes a proteção da privacidade, a segurança da informação, a integridade e a disponibilidade dos dados, reconhecendo a necessidade de garantir a confiança digital como elemento essencial à transformação dos serviços públicos.

· Decreto nº 69.052, de 14 de novembro de 2024, que atribui à Secretaria de Gestão e Governo Digital (SGGD) a responsabilidade pela coordenação da política de cibersegurança no âmbito da Administração Pública Estadual, compreendendo a prevenção, detecção, resposta e recuperação diante de incidentes cibernéticos.

· Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

· Lei Federal nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que dispõe sobre princípios, garantias, direitos e deveres para o uso da internet no Brasil, estabelecendo diretrizes quanto à proteção da privacidade e da segurança dos dados.

· Política de Aquisições para Operações Financiadas pelo Banco Interamericano de Desenvolvimento (GN-2349-15), aplicável em razão do financiamento parcial do Projeto São Paulo Mais Digital, que estabelece princípios de eficiência, transparência e integridade nas contratações públicas.

· Lei Federal nº 13.303, de 30 de junho de 2016 (Lei das Estatais), que 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, estabelecendo normas específicas para licitações e contratos celebrados por essas entidades.

· Normas e frameworks internacionais de segurança da informação, especialmente:

o NIST Cybersecurity Framework (NIST CSF), que define práticas para a identificação, proteção, detecção, resposta e recuperação diante de ameaças cibernéticas;

o Norma ISO/IEC 27001, que trata da gestão de segurança da informação;

o Norma ISO/IEC 27002, que estabelece diretrizes para a implementação de controles de segurança;

o Norma ISO/IEC 27035, que aborda a gestão de incidentes de segurança da informação.

Esses dispositivos normativos e técnicos fundamentam a necessidade de fortalecimento da segurança cibernética da Administração Pública Estadual e justificam a contratação do SOC, visando à confidencialidade, integridade disponibilidade dos serviços públicos digitais.

6. DESCRIÇÃO DA SOLUÇÃO DE TIC

A CONTRATADA será responsável pelo fornecimento de todos os componentes descritos a seguir, referentes aos Serviços do Centro de Operações de Segurança - Monitoramento de Incidentes Cibernéticos, objeto desta contratação. Esses componentes estão especificados em LOTE ÚNICO, conforme a tabela abaixo. Ainda, serão categorizados em soluções e elementos essenciais, organizados nas seguintes categorias: SERVIÇOS, TECNOLOGIA e INFRAESTRUTURA. A contratação terá duração de 12 (doze) meses.

6.1 Serviços e Quantitativos Estimados

Centro de Operações de Segurança				
ITEM	**DESCRIÇÃO**		**QTD**	**MÉTRICA**
1 - Serviço	Centro de Operações de Segurança - Monitoramento de Incidentes Cibernéticos	Monitoramento de eventos de segurança	12 Meses	Serviço / Mês
		Processo de melhoria contínua	12 Meses	Serviço / Mês
		Monitoramento de disponibilidade	12 Meses	Serviço / Mês
2 - Tecnologia	Solução SIEM / SOAR		100.000	EPS[1]
	Solução EDR (Workstation)		40.000	Unidade
	Solução EDR (Servidores)		1500	Unidade
	Solução EPM (Servidores)		1500	Unidade
	Solução Anti-Ransomware (Servidores)		1500	Unidade
	Instalação e configuração		1	Unidade
	Threat Intelligence		1	Unidade
3 – Serviço (Serviço pontual de gestão de incidente)	Serviço Técnico – N1		12 Meses	Serviço / Mês
	Serviço Técnico – N2		12 Meses	Serviço / Mês
	Serviço especializado – N2 e N3		12 Meses	Serviço / Mês
4 - Infraestrutura	Salas Físicas		2	Unidade

6.2 Serviços e Quantitativos Estimados

Este projeto visa a implementação de um **Centro de Operações de Segurança (SOC)** com foco inicial no monitoramento de incidentes

cibernéticos. O escopo compreende as seguintes áreas:

6.2.1 Centro de Operações de Segurança - Monitoramento de Incidentes Cibernéticos

Este serviço contempla o **acompanhamento contínuo (24/7)** de eventos, integrando os pilares de **monitoramento de disponibilidade (NOC)** e **resposta a incidentes (CSIRT)**. Ele incluirá a definição de características, requisitos e responsabilidades para as atividades de identificação, triagem, análise e tratamento de incidentes, além do acionamento de especialistas da SGGD.

6.2.1.1 Monitoramento Colaborativo

As atividades do SOC serão realizadas em **colaboração entre a CONTRATADA e a SGGD** . As responsabilidades serão detalhadas no plano de atuação pós-contrato, visando assegurar:

· **Execução e triagem inicial de eventos** com base em *playbooks* predefinidos, classificando incidentes por criticidade e prioridade, e encaminhando eventos relevantes aos especialistas.

· **Comunicação segura e contínua** entre as Salas de Monitoramento da CONTRATADA e da SGGD, garantindo alinhamento nas atividades, compartilhamento tempestivo de informações sobre ameaças e integração de dados para análise.

6.2.2 Soluções Tecnológicas Essenciais

O projeto prevê a implementação e operação de tecnologias de segurança cibernética cruciais:

· **Solução SIEM (Security Information and Event Management) / SOAR (Security Orchestration, Automation and Response)** : Detalhará as especificações técnicas para sua disponibilização, implementação e operação, com foco nas funcionalidades essenciais para o monitoramento contínuo, correlação de eventos, geração de alertas e resposta a incidentes de segurança. A solução deverá incorporar, de forma integrada ou complementar, capacidades de orquestração, automação e resposta a incidentes, permitindo a criação de playbooks automatizados, gestão centralizada de tickets, análise contextual de ameaças e resposta coordenada entre diferentes tecnologias de segurança.

· **Solução EDR (Endpoint Detection and Response):** Abrangerá as especificações técnicas para sua disponibilização, implementação e operação em

endpoints relevantes. Essa tecnologia é uma camada crítica de proteção para dispositivos finais, superando as limitações de antivírus tradicionais através de

monitoramento contínuo, análise comportamental e respostas automatizadas a incidentes.

· **Solução EPM (Endpoint Privilege Management):** Detalhará os requisitos para sua disponibilização, implementação e operação em *endpoints*. Essencial para o controle granular de privilégios em dispositivos finais, ela implementa o princípio do menor privilégio sem comprometer a produtividade dos usuários, utilizando elevação de privilégios, controle de aplicações, gerenciamento de políticas comportamentais e mecanismos robustos de auditoria e conformidade.

· **Solução Anti-Ransomware:** Abrangerá as especificações técnicas para sua disponibilização, implementação e operação em toda a infraestrutura tecnológica. Esta tecnologia especializada é uma camada crítica de proteção contra ataques de sequestro de dados, superando soluções tradicionais por meio de detecção avançada de comportamentos de criptografia maliciosa, proteção proativa de arquivos sensíveis, bloqueio de processos suspeitos e mecanismos automatizados de contenção e recuperação.

· **Solução Threat Intelligence:** Contemplará as especificações técnicas para sua disponibilização, implementação e operação. Esta solução, de natureza especializada, é um elemento essencial para um SOC moderno, pois vai além da mera agregação de *feeds* de ameaças, estabelecendo um ecossistema integrado de inteligência acionável capaz de aprimorar as capacidades preventivas, detectivas e reativas de segurança.

6.2.3 Soluções Complementares

· **Solução CSPM (Cloud Security Posture Management):** Abrangerá as especificações técnicas para sua disponibilização, implementação e operação em ambientes de computação em nuvem utilizados pelos órgãos e entidades. A solução deve permitir a avaliação contínua da postura de segurança na nuvem, identificando e corrigindo configurações inadequadas, riscos de conformidade e vulnerabilidades em recursos cloud. Deverá oferecer visibilidade centralizada, análise de riscos baseada em políticas, mecanismos automatizados de remediação e integração com outras soluções de segurança, como SIEM e SOAR, promovendo uma gestão proativa de riscos em ambientes multi-nuvem.

· **Solução WAF (Web Application Firewall):** Abrangerá as especificações técnicas para sua disponibilização, implementação e operação em aplicações web críticas. A solução deve oferecer proteção contra ataques direcionados à camada de aplicação, como injeção de SQL, XSS, exploração de vulnerabilidades conhecidas e negação de serviço. Deverá suportar inspeção profunda de pacotes HTTP/HTTPS, mitigação baseada em políticas adaptativas, modelos de aprendizado de comportamento de aplicação, proteção contra bots maliciosos e integração com plataformas de Threat Intelligence e SIEM, possibilitando resposta coordenada a ameaças em tempo real.

· **Solução Pentest (Teste de Intrusão):** Abrangerá as especificações técnicas para a contratação e execução periódica de testes de intrusão em aplicações, redes e infraestrutura crítica. Esse serviço tem como objetivo identificar vulnerabilidades técnicas e lógicas que possam ser exploradas por agentes mal-intencionados, simulando ataques controlados com diferentes níveis de acesso (caixa preta, cinza e branca). A execução dos testes deverá gerar relatórios técnicos e executivos com evidências, análises de risco, recomendações de correção e avaliação da eficácia das soluções de segurança implementadas, como EDR, WAF, SIEM e SOAR.

6.2.4 Serviço Pontual de Resposta a Incidentes

Serão destacadas as características esperadas e os quantitativos estimados para atendimento de demandas pontuais de resposta a incidentes.

6.2.5 Salas Físicas

Contemplará as características e especificações técnicas para o fornecimento de equipamentos, montagem, instalação, operação e manutenção das salas físicas do Centro de Operações de Segurança.

ITEM 1. Requisitos dos serviços técnicos especializados do centro de monitoramento de incidentes cibernéticos.

O Serviço de monitoramento de incidentes cibernéticos deverá realizar em tempo real, o monitoramento, a análise e o escalonamento de eventos de segurança, garantindo rastreamento contínuo, a emissão de alertas iniciais e o encaminhamento tempestivo às equipes de “Serviço Pontual de Respostas a Incidentes” ou “Especialistas Integrados à SGGD”, no caso de potenciais incidentes. Essas atividades compreendem:

ITEM 1.1 Requisitos dos serviços monitoramento de eventos de segurança.

O Centro de Monitoramento de Eventos de Segurança tem como objetivo principal a detecção proativa e a resposta eficiente a incidentes

cibernéticos. Para isso, a equipe deverá identificar atividades suspeitas e anomalias em tempo real, utilizando ferramentas avançadas como SIEM e XDR para elaborar queries e scripts que permitam o rastreamento, refinamento das investigações e a correlação de eventos.

A gestão desses eventos exige que a equipe monitore, intérprete e análise alertas gerados pelo sistema SIEM e pela plataforma XDR, garantindo a correta abertura de tickets a partir das ferramentas ITSM (ServiceNow) definidas pelo CONTRATANTE, com categorização adequada para priorização e tratamento. Esta etapa inclui a realização de investigação inicial de alertas e incidentes provenientes de sistemas SIEM (Event Management) e soluções de proteção de endpoints, aplicando as práticas recomendadas para identificação de padrões de ataque e correlação de eventos.

A identificação, correlação e priorização de eventos de segurança basear-se-ão em regras de negócios personalizadas para o ambiente do CONTRATANTE, políticas internas de cibersegurança e frameworks de ameaças e Técnicas, Táticas e Procedimentos (TTPs) reconhecidos, como MITRE ATT&CK, Cyber Kill Chain e NIST-CSF. Paralelamente, será crucial analisar, contextualizar e fornecer insights de criticidade para IPs, hashes, URLs e IoCs externos, possibilitando desafios ou bloqueios automáticos quando permitido, sempre com base em inteligência de ameaças confiável.

O monitoramento se estende à investigação de logs de segurança de sistemas, redes e aplicativos críticos, identificando anomalias, padrões suspeitos e variações atípicas de comportamento em tempo real, com o uso de análise contextual e detecção avançada de ameaças emergentes. Haverá um monitoramento contínuo dos eventos capturados pelo IPS (*Intrusion Prevention System*), priorizando alertas de alto risco como tentativas de exploração de vulnerabilidades conhecidas, ataques de negação de serviço (DoS/DDoS) e atividades maliciosas baseadas em rede. A equipe também monitorará alertas gerados pelas operadoras de infraestrutura de conectividade, correlacionando-os com eventos internos para confirmar a presença e a criticidade de possíveis ataques DDoS, e validará o desempenho de soluções anti-DDoS internas da SGGD na identificação e mitigação de tráfegos maliciosos.

A correlação de telemetrias geradas por soluções de segurança como EDR, antivírus, ATP, Proxy, Firewalls, IPS, Antispam e scanners de vulnerabilidades é vital para otimizar a visibilidade de ataques avançados e permitir a mitigação proativa. As plataformas devem, preferencialmente, enviar alertas ao SIEM para centralização e análise contínua. Eventos de comportamento anômalo serão monitorados e documentados utilizando IoCs, TTPs conhecidos e regras YARA, alinhados à inteligência de ameaças global e local.

As informações complementares obtidas no SIEM serão correlacionadas e validadas com dados de outros sistemas ou logs da infraestrutura interna, proporcionando uma análise mais ampla e detalhada para investigação avançada pelas equipes de resposta. O monitoramento e análise contínuos de eventos detectados por soluções de EDR/XDR incluirá a correlação de dados entre endpoints, rede e outras camadas de segurança para maior precisão na identificação de ameaças avançadas. Os alertas serão validados em tempo real, utilizando análises contextuais e técnicas baseadas em TTPs documentados no MITRE ATT&CK, alinhando-os ao ambiente protegido.

Serão realizadas análises de comportamento em endpoints em busca de anomalias ou padrões de ataque, utilizando inteligência artificial (IA) e aprendizado de máquina (ML – *machine learning*) para prever e mitigar ameaças antes da execução. A correlação de informações de EDR/XDR com plataformas SIEM e SOAR permitirá a geração de relatórios analíticos, dashboards e dados centralizados, facilitando a identificação e priorização de ameaças críticas.

A equipe deverá implementar e customizar playbooks automatizados no XDR para responder a cenários de ataques específicos, como campanhas de ransomware, tentativas de exploração de vulnerabilidades conhecidas e execução de malware ou scripts maliciosos. Além disso, a gestão de incidentes envolverá abrir, gerenciar e acompanhar tickets em ferramentas ITSM (ServiceNow) para todos os eventos de DoS registrados, garantindo controle do fluxo de tratamento até a resolução ou escalonamento para as equipes de resposta.

A atualização de listas de bloqueio ou permissão relacionadas a IPs ou URLs específicas será realizada, garantindo a sincronização com as ferramentas de monitoramento e Listas de Controle de Acesso (ACLs) utilizadas. A verificação da reputação de Autonomous Systems (AS) relacionados a ataques será feita com validação em bases externas e feeds de inteligência de ameaças, identificando potenciais agentes maliciosos.

O monitoramento, registro e análise do tráfego web extraído da solução de proxy permitirá identificar acessos maliciosos, tentativas de acesso a sites de alto risco, conteúdo potencialmente inadequado e atividades anômalas. Mensagens analisadas por soluções de proteção de e-mails e anti-spam serão continuamente monitoradas, detectando padrões de e-mails maliciosos como phishing, spear phishing, spoofing e e-mails com anexos ou links maliciosos.

O monitoramento e análise contínuos de alertas gerados pelas soluções de ATP (Advanced Threat Protection) focarão na identificação e resposta a ameaças avançadas, como ransomware, ataques de dia zero e tentativas de exploração de vulnerabilidades críticas. A análise comportamental em tempo real e a correlação de eventos suspeitos capturados por soluções ATP com dados de outras ferramentas (SIEM, SOAR, XDR) serão cruciais para identificar campanhas avançadas e coordenadas.

A automação da coleta e análise em tempo real de Indicadores de Comprometimento (IoCs) e Indicadores de Ataque (IoAs) capturados garantirá o bloqueio preventivo em toda a infraestrutura corporativa. Os dados de tráfego do proxy serão correlacionados com informações de SIEM, SOAR e XDR para criar uma visão centralizada e detectar padrões de ataques direcionados.

Testes periódicos e auditorias das políticas configuradas em ferramentas de proteção de e-mails identificarão lacunas e assegurarão conformidades regulatórias, como LGPD ou GDPR. Análises preditivas utilizando inteligência artificial (IA) e machine learning (ML) serão incorporadas para antecipar potenciais incidentes e apresentar previsões baseadas em comportamentos anômalos. Eventos de comportamento anômalo serão monitorados e documentados com regras YARA, IoCs e TTPs conhecidos, fortalecendo as capacidades preditivas e responsivas do SOC.

A equipe deverá fornecer análises detalhadas sobre as ameaças detectadas por EDR/XDR, incluindo a cadeia completa do ataque (Kill Chain), métodos de entrada e propagação, impacto potencial nos sistemas e mitigação adotada, e possíveis falhas ou gaps a serem corrigidos para evitar reincidências. Contribuirá para melhorias contínuas na configuração das soluções EDR/XDR, ajustando políticas e regras de detecção com base em ameaças globais e lições aprendidas. Modelos de detecção de ameaças customizados serão criados e ajustados.

A elaboração e revisão da documentação, incluindo playbooks e manuais de procedimentos do Centro de Monitoramento, promoverá a padronização e a melhoria contínua. Relatórios analíticos e periódicos serão desenvolvidos, abrangendo o número de acessos bloqueados por categoria de ameaça, domínios e IPs recusados, padrões de navegação inadequados/anômalos, e indicadores-chave (taxa de detecções falsas e acertos na aplicação de políticas).

Playbooks específicos serão desenvolvidos para resposta a classes de ameaças identificadas por ATP (ex: ransomwares com evasão, spear phishing coordenado) e para cenários de ataque do IPS (ex: network-based, zero- day, C2, força-bruta). Mensagens enviadas serão monitoradas para alertas automáticos de atividades suspeitas (ex: spam, mensagens fraudulentas de contas comprometidas). As ferramentas de proteção de e-mails validarão automaticamente a autenticidade das mensagens recebidas usando SPF, DKIM e DMARC.

Será oferecido apoio em campanhas regulares de conscientização e treinamento para usuários e gestores sobre ataques de e-mail, incluindo simulações de phishing e relatórios personalizados. A equipe auxiliará na configuração e atualização contínua de regras de bloqueio e políticas de proteção em soluções de segurança, baseadas em IoCs e melhores práticas. As políticas de segurança, especialmente de e-mail,

e ajustes proativos em ferramentas anti- phishing serão auditados continuamente para reduzir falsos positivos e otimizar.

Eventos detectados pelo IPS serão correlacionados com dados de ferramentas integradas (SIEM, SOAR, XDR) para análise contextualizada. Auditorias periódicas nas regras do IPS otimizarão a detecção e reduzirão falsos positivos. As métricas de desempenho do IPS (taxa de detecção de incidentes, falsos positivos, impacto na rede) serão constantemente monitoradas.

Auditorias frequentes nas políticas e configurações das soluções ATP otimizarão o balanceamento entre proteção e desempenho, reduzindo falsos positivos. As integrações com EDR serão exploradas para ampliar análises e permitir respostas detalhadas (ex: isolamento de endpoints). Alertas automáticos para acessos suspeitos (C2, malware, phishing) serão implementados e escalados.

Auditorias frequentes nas ACLs de soluções de proxy manterão os bloqueios de URLs, IPs ou categorias desnecessárias atualizados. As assinaturas e regras do IPS serão configuradas e mantidas atualizadas com bases de dados de fabricantes e inteligência de ameaças. As soluções ATP serão continuamente atualizadas com inteligência de ameaças em tempo real.

As tentativas de phishing serão continuamente monitoradas por soluções de proteção de e-mail e ferramentas de análise comportamental. Novos vetores de ataques de phishing (ex: spear phishing, credential harvesting, smishing, vishing) serão identificados e combatidos. Os dados de phishing detectados serão correlacionados com plataformas de SIEM e ferramentas de inteligência de ameaças para identificar padrões recorrentes e prever novas campanhas.

Por fim, a transição fluida de turnos será garantida, com relatórios de follow-ups detalhados, assegurando a continuidade operacional e a rastreabilidade das ações. Além disso, será garantida a criação de uma base de conhecimento interna com reportes regulares sobre incidentes de phishing detectados, lições aprendidas e estatísticas. Processos de coleta e análise detalhada de IoCs de phishing serão implementados para bloqueio preventivo de domínios. Todos os incidentes de segurança serão escalados conforme o Plano de Escalonamento definido.

ITEM 1.2 Requisitos dos processos de melhoria contínua

O Centro de Monitoramento de Incidentes Cibernéticos terá um papel proativo na evolução e aprimoramento contínuo das capacidades de detecção e resposta a ameaças. Isso se manifestará através do desenvolvimento e implementação de planos estratégicos voltados para aumentar a taxa de detecção e a eficiência na resposta, buscando reduzir o Tempo Médio para Contenção e Mitigação (MTTR) por meio de processos automatizados. Tais planos deverão incluir a customização de modelos de detecção alinhados às necessidades específicas do contratante, além da sugestão de novos modelos baseados em padrões de ataques globais e emergentes.

A equipe será responsável por propor melhorias contínuas nos fluxos de trabalho e na integração de novos recursos, como a inteligência de ameaças cibernéticas, nas soluções de segurança do ambiente. O objetivo é acelerar a triagem e a priorização dos eventos reportados. Adicionalmente, serão propostas, documentadas e implementadas melhorias contínuas nas metodologias de triagem, visando a redução de falsos positivos, a consolidação e priorização de eventos, e a criação e ajuste de novas regras de correlação e detecção, integrando-as às plataformas SIEM.

O monitoramento contínuo do ambiente de segurança será realizado para identificar possíveis gaps ou vulnerabilidades, propondo ações corretivas e melhorias em colaboração com as equipes de "Serviço Pontual de Respostas a Incidentes" ou "Especialistas Integrados à SGGD". Para garantir a eficácia operacional, a equipe deverá acompanhar e analisar indicadores de segurança cibernética relacionados à expansão ou alterações no inventário de ativos protegidos pelo SOC, reportando divergências ou anomalias identificadas para investigação detalhada.

A integração contínua entre as plataformas de segurança (SIEM, SOAR, XDR e outras) será uma prioridade, com o ajuste de configurações e regras para melhorar a eficiência na detecção e resposta a incidentes. A equipe também realizará análises de tendências e padrões de eventos de segurança, propondo ajustes proativos em regras de detecção e correlação para antecipar possíveis ameaças.

No que tange à automação, o serviço apoiará iniciativas de automação de tarefas rotineiras por meio de soluções de segurança, promovendo maior eficiência no tratamento de incidentes e a consequente redução do tempo de resposta.

As políticas de segurança serão continuamente revisadas e aprimoradas:

· Serão propostas ações preventivas e melhorias contínuas em playbooks e procedimentos de tratamento de DDoS, baseando-se em dados observados durante incidentes passados, tendências globais de ataques volumétricos e novas táticas (como amplificação, reflexão e ataques lentos), além de ajustes às políticas de escalonamento.

· Serão propostas melhorias contínuas nas políticas de bloqueio e monitoramento da plataforma de XDR, ajustando estratégias de detecção e resposta com base nas lições aprendidas de incidentes reportados, resultados de análises de ameaças críticas e integrações com outras ferramentas como SIEM, SOAR e EDR.

· Serão propostas melhorias contínuas nas políticas de proxy e filtro de conteúdo, fundamentadas em tendências de ameaças emergentes, inteligência de ameaças e relatórios de acessos bloqueados.

· Serão propostos ajustes contínuos nas políticas de antispam, com base na análise de dados de ameaças detectadas globalmente, incluindo a criação de allowlists e blocklists personalizadas para aumentar a precisão dos filtros.

ITEM 1.3 Requisitos dos serviços de monitoramento de disponibilidade

O Centro de Monitoramento de Incidentes Cibernéticos garante a continuidade operacional e a integridade dos dados através do monitoramento constante da infraestrutura de segurança. A equipe será responsável por verificar continuamente o status dos coletores de eventos (Data Collectors), alertando o “Serviço Pontual de Respostas a Incidentes” ou os “Especialistas Integrados à SGGD” em caso de falhas, interrupções ou degradação de performance, para assegurar a fluidez do fluxo de dados.

Adicionalmente, será realizado o monitoramento de disponibilidade de todas as soluções de segurança que fazem parte do escopo do serviço de monitoramento de incidentes cibernéticos. Isso inclui, mas não se limita, ao acompanhamento dos recursos e desempenho da solução interna anti-DDoS, com foco em aspectos críticos como o consumo de CPU, memória e largura de banda da solução. Também serão observadas as taxas volumétricas de pacotes ou tráfego (PPS/Gbps) anômalos, bem como os eventos de bloqueios automáticos e manuais gerados pela ferramenta, garantindo a eficácia na proteção contra ataques de negação de serviço.

ITEM 1.4 Requisitos dos serviços de confecção / criação de relatórios

A capacidade de gerar relatórios abrangentes e informativos é fundamental para o Centro de Monitoramento de Eventos de Segurança. A equipe será responsável por elaborar relatórios de eventos detectados com informações completas, detalhando os eventos identificados e categorizados, os dados correlacionados a partir de plataformas SIEM e XDR, e os Indicadores de Comprometimento (IoCs) e Técnicas, Táticas e Procedimentos (TTPs) identificados.

Serão gerados relatórios estruturados sobre incidentes detectados, triados e tratados, incluindo métricas essenciais como o Tempo Médio de Detecção (MTTD), Tempo Médio de Resposta (MTTR) e a taxa de falsos positivos. Esses relatórios darão visibilidade aos principais tipos de eventos detectados e sua evolução (tendências e padrões), comparando-os a tentativas de ataques globais ocorridas no mesmo período,

utilizando referências de inteligência de ameaças (Threat Intelligence).

Para uma visão holística, a equipe deverá consolidar dados de múltiplas ferramentas e plataformas, como SIEM, SOAR, XDR e soluções anti-DDoS, para criar relatórios que incluam tráfego malicioso detectado e bloqueado, a evolução de eventos por tipo (phishing, malware, exploits, etc.) e a comparação entre eventos internos e ataques globais.

Os relatórios serão criados em diferentes níveis de abstração para atender a públicos específicos:

· Operacional: com detalhes técnicos e métricas de desempenho.

· Gerencial: oferecendo um resumo estratégico, gráficos e análise de impacto operacional.

· Executivo: apresentando apontamentos de alto nível para auxiliar na tomada de decisão estratégica. Relatórios periódicos e especializados

A equipe elaborará relatórios periódicos detalhados sobre a eficiência da solução de antispam, cobrindo o número de mensagens bloqueadas e os motivos, os principais remetentes e domínios de alto risco, análises de campanhas de phishing detectadas e mitigadas, e os resultados de simulações conduzidas internamente.

Também serão produzidos relatórios periódicos detalhados sobre os eventos monitorados em geral, incluindo volume de alertas tratados, taxa de falsos positivos, indicadores de desempenho (MTTD, MTTR) e recomendações para aprimoramento contínuo das operações de segurança. Relatórios periódicos sobre ataques DDoS detalharão o volume e frequência de ataques detectados, os principais IPs e ASs ofensores, a efetividade das ações de mitigação e recomendações para aprimorar a resiliência contra ataques futuros.

Análise de tendências e relatórios pós-incidente

Os relatórios incorporarão insights relevantes da análise de tendências, como as principais vulnerabilidades exploradas, ameaças emergentes detectadas e os tipos de ataques mais frequentes e evasões observadas. Após incidentes, serão gerados relatórios pós-incidente detalhados (Post-Incident Review), contemplando a linha do tempo do evento, sua origem e impacto, as ações corretivas e preventivas executadas, as lições aprendidas e recomendações para evitar reincidências.

Personalização, segurança e automação dos relatórios

A equipe terá a capacidade de oferecer relatórios personalizados para atender a requisitos específicos do contratante, como auditorias e acompanhamento de conformidades regulatórias baseadas em normas e frameworks, por exemplo, LGPD, ISO/IEC 27001 ou NIST-CSF. Todos os relatórios deverão atender aos requisitos de segurança e privacidade, adotando medidas de proteção como criptografia e controle de acesso, para evitar vazamentos ou acessos não autorizados a informações sensíveis.

Para otimizar a entrega, a geração e o envio periódico de relatórios serão automatizados utilizando integrações com SOAR ou ferramentas similares via agendamento predefinido, reduzindo esforços operacionais e garantindo a conformidade com SLAs. Complementando os relatórios estáticos, serão desenvolvidos dashboards interativos e dinâmicos que permitam a visualização em tempo real dos principais indicadores e eventos de segurança, utilizando ferramentas de BI ou dashboards integrados ao SIEM e SOAR.

Eficácia e desempenho operacional

A equipe deverá documentar e analisar a eficácia das respostas aos eventos detectados, destacando ações que podem ser otimizadas ou automatizadas para reduzir o tempo de resposta e aumentar a eficiência geral do processo. Isso inclui o desenvolvimento de relatórios de desempenho e indicadores-chave (KPIs), como Tempo Médio de Detecção (MTTD), Tempo Médio de Resposta (MTTR), taxa de falsos positivos, e volume de incidentes tratados e mitigados.

Relatórios de desempenho específicos para EDR/XDR incluirão métricas como taxas de detecção e prevenção, Tempo Médio de Resposta (MTTR), volume de incidentes resolvidos automaticamente, e a redução de exposição a riscos baseada nas ações tomadas. Serão elaborados relatórios periódicos sobre ameaças detectadas e mitigadas, consolidando indicadores como tipos e volumes de ameaças bloqueadas, cadeias completas de ataques observados (Kill Chain), e recomendações para evitar recorrência e corrigir brechas identificadas.

Além disso, serão desenvolvidos relatórios periódicos detalhados para oferecer visibilidade sobre os principais tipos e volumes de ameaças detectadas, identificar padrões frequentes de ataque e apresentar as principais ações preventivas e corretivas tomadas. Serão elaborados também relatórios periódicos detalhando estatísticas de phishing detectado e bloqueado, taxa de participação e sucesso em campanhas de simulação de phishing, indicadores de eficácia das respostas automatizadas e ajustes realizados nas ferramentas após ocasiões de ataques.

Para o tratamento inicial de ameaças confirmadas, a equipe deverá executar o primeiro atendimento e realizar ações iniciais de contenção para incidentes padrão, com base em playbooks automatizados ou manuais. Casos que exigirem análise avançada ou resposta especializada serão escalonados para o “Serviço Pontual de Respostas a Incidentes” ou “Especialistas Integrados à SGGD”, conforme o modelo de atendimento multinível.

ITEM 1.5 Propriedade intelectual e titularidade de artefatos

Todos os dados, artefatos, relatórios, playbooks, dashboards, scripts, configurações e demais ativos produzidos ou customizados no âmbito da prestação dos serviços contratados pertencem exclusivamente à Secretaria de Gestão e Governo Digital (SGGD), sendo vedada sua reutilização pela CONTRATADA fora do escopo do presente contrato.

Deverá ser garantido acesso integral e irrestrito à documentação técnica, aos repositórios de artefatos e aos registros gerados, incluindo aqueles utilizados em soluções SIEM, SOAR, EDR, XDR e correlatos, inclusive em caso de encerramento contratual. A entrega destes artefatos poderá ser demandada a qualquer tempo pela SGGD.

ITEM 2. Requisitos funcionais das soluções ITEM 2.1 Requisitos funcionais da solução SIEM

A solução SIEM (Security Information and Event Management) deve ser uma plataforma robusta e eficiente, capaz de otimizar a detecção, análise e resposta a incidentes de segurança.

Coleta e normalização de eventos

A plataforma deve garantir a coleta, normalização e correlação de eventos provenientes dos dispositivos monitorados em tempo próximo ao real. Todos os eventos precisam ser normalizados e categorizados em um padrão único para uso consistente na solução. Será fundamental permitir a definição de metadados customizados e personalizados, extraindo dados da linha de log (raw) através de recursos como expressões regulares ou ferramentas gráficas. Essas propriedades customizadas deverão ser aplicáveis tanto em regras de correlação online quanto em regras de correlação histórica. A solução também deve possibilitar a agregação de eventos semelhantes para otimização do volume de dados.

A solução SIEM deverá ter, no mínimo, as seguintes formas de coleta de eventos para garantir a abrangência necessária:

· Protocolos de log padrão: Syslog (UDP, TCP, e criptografado com TLS), JDBC e SNMP (v1, v2 e v3).

· Sistemas operacionais e plataformas: Microsoft Event Log.

· Mensageria e streaming: MQ Series cliente, Kafka, AWS Kinesis, Azure Event Hubs e Google Cloud Pub/Sub.

· Fontes de armazenamento em nuvem: AWS S3 e AWS Cloudwatch.

· Dispositivos e appliances de segurança: Checkpoint OPSEC/LEA e CISCO NSEL.

· Outros: Arquivos de Log em formato de texto e API REST genérica.

· Networking: Juniper NSM Protocol. Processamento e armazenamento de dados

A solução deve ser capaz de processar logs em diversos formatos, como JSON, CEF, LEEF, XML e Chave/Valor, identificando e criando automaticamente os campos comuns do log como metadados. Para formatos como JSON, XML, Chave/Valor e CSV, a plataforma deve permitir a definição manual/customizada de metadados utilizando a estrutura/caminho do JSON, tag XML, posição no CSV ou chave do Chave/Valor. Além disso, deverá ser possível definir metadados customizados/personalizados para extrair dados de uma linha de log (raw) usando recursos como expressões regulares, JSON, LEEF, XML, Chave/Valor, CSV e CEF, a partir de dados RAW previamente armazenados, permitindo o uso desses dados em pesquisas de eventos. A capacidade de sugerir expressões regulares para identificar porções do log selecionadas graficamente para criação/edição de metadados customizados é um diferencial. A criação de metadados com nomes personalizados de livre escolha, permitindo a referência em pesquisas e regras de correlações, também é um requisito.

Os eventos, inclusive os normalizados, devem ser armazenados de forma compactada. A solução deve permitir o armazenamento e a retenção de logs por um período mínimo de 12 meses, com possibilidade de extensão por até 5 anos, conforme critérios e diretrizes a serem definidos pela SGGD, em conformidade com requisitos legais, regulatórios e de auditoria.

Análise, alertas e conformidade

É essencial que a solução atribua uma métrica de prioridade para os eventos e para os alertas/incidentes gerados, com base nas regras previamente definidas. Deve-se permitir a análise de eventos baseada em contexto, considerando fatores como usuários, localização geográfica e qualquer outro metadado contido no evento.

A plataforma precisa gerar alertas/incidentes com base nas regras de correlação definidas, e enviar notificações relacionadas por e-mail, trap SNMP e syslog. A visualização, na interface web, dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução é crucial para a investigação. Além disso, a SIEM deve verificar a conformidade com políticas, controles e normas internas (customizadas) e regulamentações externas (ex: ISO 27001, PCI, SOX, HIPAA).

Gerenciamento de incidentes e resposta automatizada

A solução deverá ser fornecida com um módulo integrado para o gerenciamento dos incidentes identificados. Para acelerar a resposta, deve possuir a capacidade de automatizar a resposta a incidentes através da execução de scripts como ação customizada dentro das regras de correlação. Também será necessário customizar e personalizar diferentes "templates" de e-mail que serão enviados como resposta aos incidentes identificados.

Integração e saída de dados

A solução deve ter a capacidade de reenviar os logs e flows, em formato nativo, para outros sistemas em tempo real, e também reenviar eventos já normalizados para outros sistemas de correlacionamento em tempo real. A configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados, é um requisito de segurança, sendo que a ofuscação de dados deve ser configurada com chaves de criptografia.

Visualização e usabilidade

Para facilitar a análise, a solução deve apresentar painéis gráficos (dashboards) com indicativos de situações relacionadas à segurança, compliance, aplicações e monitoração do próprio sistema. Esses dashboards deverão ser customizáveis por usuário, garantindo uma experiência personalizada e eficiente para cada analista ou gestor.

ITEM 2.2 Requisitos Funcionais da Solução EDR

A solução EDR (Endpoint Detection and Response) é fundamental para proteger os endpoints da organização, oferecendo visibilidade e capacidade de resposta avançadas.

Detecção e visibilidade abrangente

A coleta, análise e correlacionamento de eventos e comportamentos nos endpoints devem ser realizados em tempo real, com latência mínima. A solução deve fornecer visibilidade completa sobre processos em execução, modificações de registro, conexões de rede, operações de arquivo e atividades de usuário em todos os endpoints monitorados.

A detecção de ameaças deve ocorrer através de múltiplos métodos, incluindo análise comportamental, machine learning, Indicadores de Comprometimento (IoCs) e regras de detecção personalizáveis. A solução precisa identificar e alertar sobre técnicas de ataque mapeadas no framework MITRE ATT&CK, abrangendo execução de código malicioso, persistência, escalação de privilégios, evasão de defesas, acesso a credenciais, movimentação lateral e exfiltração de dados.

Capacidades de resposta remota

A solução EDR deve oferecer capacidades de resposta remota robustas, incluindo, no mínimo:

· Isolamento de rede do endpoint comprometido.

· Encerramento de processos maliciosos.

· Remoção de arquivos maliciosos.

· Coleta de evidências forenses.

· Quarentena de arquivos suspeitos. Investigação forense e Threat Hunting

A plataforma deve fornecer investigação forense detalhada, que contemple uma timeline completa de eventos, visualização gráfica da cadeia de ataque e reconstrução de incidentes. Além disso, deve permitir a busca retrospectiva (hunting) em dados históricos para identificação de ameaças previamente não detectadas, utilizando novos indicadores ou regras.

Priorização, integração e usabilidade

A solução precisa permitir a categorização e priorização de alertas com base em criticidade, impacto potencial e contexto do ambiente. A integração nativa com a solução SIEM é essencial, permitindo o envio de alertas, eventos e metadados contextuais. Da mesma forma, deve possibilitar a integração com soluções SOAR para orquestração e automação da resposta a incidentes.

Para monitoramento e gestão, a solução deve oferecer dashboards personalizáveis com métricas de segurança, status de endpoints, alertas ativos e tendências de ameaças.

Gerenciamento de políticas e operação offline

A solução deve suportar a implementação de políticas de segurança baseadas em grupos de endpoints, perfis de usuários e níveis de sensibilidade. É crucial que a solução opere mesmo quando o endpoint estiver offline, mantendo capacidades de detecção e resposta locais.

Deve suportar a implementação de listas de permissão (allowlist) e bloqueio (denylist) de aplicações, processos e comportamentos. Além disso, deve permitir a coleta sob demanda de artefatos forenses dos endpoints para análise detalhada, incluindo memória RAM, arquivos de sistema e registros.

Escaneamento de vulnerabilidades e controle de dispositivos

A solução EDR deve oferecer capacidade de escaneamento e remediação de vulnerabilidades nos endpoints, com priorização baseada em exploração ativa. Deve também permitir a configuração de políticas de controle de dispositivos (USB, periféricos) e controle de aplicações.

Segurança e compatibilidade

Para a administração, a solução deve suportar autenticação multifator para acesso ao console de gerenciamento e implementar controle de acesso baseado em funções (RBAC). Além disso, deve manter logs detalhados de todas as ações administrativas e operacionais para fins de auditoria e conformidade.

A compatibilidade é um requisito chave, e a solução deve ser compatível com os principais sistemas operacionais do ambiente, incluindo:

· Windows: 7, 8, 10, 11, Server 2012 R2, 2016, 2019, 2022.

· Linux: principais distribuições enterprise.

· macOS: as três versões mais recentes.

Por fim, a solução deve suportar a exportação de dados em formatos padrão (CSV, JSON, PDF) para integração com ferramentas de análise externas, e permitir a criação de fluxos de trabalho customizados para tratamento de incidentes, com atribuição de responsabilidades e prazos.

ITEM 2.3 Requisitos Funcionais da Solução EPM

A solução EPM (Endpoint Privilege Management) visa implementar o princípio do menor privilégio, garantindo segurança sem comprometer a produtividade do usuário.

Gerenciamento de privilégios e controle de aplicações

A solução deve implementar o princípio de menor privilégio nos endpoints, permitindo que usuários operem com contas padrão (não-administradores) para tarefas cotidianas. Deve permitir a elevação de privilégios contextual e granular para aplicações específicas, sem conceder direitos administrativos completos ao usuário. A criação de políticas de elevação de privilégios baseadas em grupos de usuários, departamentos, funções e níveis de sensibilidade dos endpoints é essencial.

A solução precisa implementar listas de permissão (allowlist) e bloqueio (denylist) para aplicações, scripts e comandos, com capacidade de atualização automática. Deve oferecer proteção contra técnicas de bypass de UAC (User Account Control) e outras técnicas de escalação de privilégios.

Monitoramento, auditoria e gravação de sessões

A solução deve oferecer capacidade de monitoramento e auditoria detalhada de todas as atividades privilegiadas, incluindo comandos executados, aplicações iniciadas com privilégios elevados, modificações em arquivos e registros do sistema, e tentativas de violação de políticas. Além disso, deve permitir a gravação de sessões privilegiadas para fins de auditoria e investigação forense.

Controle de scripts e regras temporárias

Será fundamental que a solução implemente controle granular sobre scripts PowerShell, VBScript, Python e outros, permitindo a execução controlada com base em conteúdo, origem e comportamento. Deve permitir a criação de regras de elevação temporárias para casos específicos, com expiração automática após um período determinado.

Fluxos de aprovação e autoaprovação

A solução deve implementar fluxos de aprovação para solicitações de elevação de privilégios, com múltiplos níveis de aprovação configuráveis. Deve oferecer capacidade de autoaprovação para aplicações específicas, com justificativa obrigatória e registro de auditoria.

Integração, visibilidade e conformidade

A solução precisa permitir a integração com sistemas de gerenciamento de identidades e diretórios corporativos (Active Directory, Azure AD, LDAP). Para a gestão, deve oferecer dashboards personalizáveis com métricas de segurança, status de endpoints, tentativas de violação de políticas e tendências de uso.

A geração de relatórios detalhados para fins de conformidade com regulamentações (PCI-DSS, ISO 27001, LGPD) é um requisito.

Segurança da plataforma e compatibilidade

Para a administração da plataforma, deve implementar controle de acesso baseado em funções (RBAC). A solução precisa oferecer capacidade de operação offline, mantendo políticas de elevação mesmo quando o endpoint estiver desconectado. Deve permitir a integração nativa com soluções SIEM, EDR e SOAR para correlacionamento de eventos e resposta a incidentes.

A solução deve oferecer proteção contra modificações não autorizadas de suas configurações e componentes. Será necessário permitir a implementação de políticas baseadas em localização geográfica e contexto de rede (corporativa, pública, VPN).

Descoberta, análise comportamental e controle avançado

A solução deve oferecer capacidade de descoberta e inventário de aplicações que requerem privilégios elevados no ambiente. Deve permitir a criação de políticas baseadas em análise comportamental e machine learning para identificação de padrões anômalos de uso de privilégios. A solução deve implementar controle sobre instalação e execução de drivers e serviços privilegiados.

Adicionalmente, deve oferecer proteção contra técnicas de injeção de código e DLL hijacking e permitir a criação de sandboxes para execução isolada de aplicações não confiáveis.

A compatibilidade com os principais sistemas operacionais do ambiente é crucial, incluindo:

· Windows: 10, 11, Server 2016, 2019, 2022.

· Linux: principais distribuições enterprise.

· macOS: as três versões mais recentes.

Por fim, a solução deve oferecer um console de gerenciamento centralizado com capacidade de administração baseada em web. Deve ter capacidade de integração com ferramentas de gerenciamento de vulnerabilidades para priorização de controles baseados em riscos e

permitir a exportação de dados em formatos padrão (CSV, JSON, PDF) para integração com ferramentas de análise externas.

ITEM 2.4 Requisitos Funcionais da Solução Anti-Ransomware

A solução Anti-Ransomware é vital para prover proteção robusta e multicamadas contra ataques de sequestro de dados em toda a infraestrutura.

Detecção e prevenção multicamadas

A solução deve oferecer proteção em tempo real contra ataques de ransomware, utilizando múltiplas camadas de detecção e prevenção. Ela precisa implementar análise comportamental avançada para identificação de padrões de criptografia maliciosa e atividades suspeitas relacionadas a ransomware. Para combater ameaças emergentes, a solução deve utilizar tecnologias de machine learning e inteligência artificial para detecção de variantes de ransomware desconhecidas e ataques zero-day.

A proteção deve se estender a técnicas de movimento lateral utilizadas em ataques de ransomware direcionados. A solução deve implementar monitoramento contínuo de atividades de arquivos, detectando padrões anômalos de:

· Renomeação em massa.

· Modificação de tipos de arquivo.

· Alterações em cabeçalhos de arquivos.

· Operações de criptografia não autorizadas.

· Exclusão de shadow copies e backups. Bloqueio, proteção proativa e recuperação

A solução deve oferecer capacidade de bloqueio automático de processos suspeitos antes que a criptografia de arquivos seja iniciada. Será fundamental a implementação de proteção proativa para arquivos críticos e sensíveis, impedindo modificações não autorizadas. Em caso de ataque, a solução deve oferecer capacidade de rollback de arquivos afetados, utilizando cópias temporárias ou snapshots locais.

Proteção contra técnicas de ataque específicas

A plataforma deve implementar proteção contra técnicas de exploração de vulnerabilidades comumente utilizadas em ataques de ransomware. A proteção também deve cobrir ataques de ransomware baseados em scripts (PowerShell, VBScript, JavaScript, etc.) e técnicas de ofuscação e evasão utilizadas por ransomware avançado.

A solução deve implementar proteção contra ransomware que utiliza técnicas de criptografia legítima do sistema operacional e ataques que exploram ferramentas legítimas (living-off-the-land). A proteção contra técnicas de desativação de soluções de segurança também é um requisito. Além disso, deve oferecer capacidade de detecção e bloqueio de comunicações com servidores de comando e controle (C2) utilizados em ataques de ransomware e implementar proteção contra técnicas de exfiltração de dados usadas em ataques de ransomware de dupla extorsão.

Análise forense e regras personalizadas

A solução deve oferecer capacidade de análise forense detalhada após tentativas de ataque, incluindo:

· Processos envolvidos.

· Arquivos afetados ou que seriam afetados.

· Vetores de entrada.

· Técnicas utilizadas.

· Indicadores de Comprometimento (IoCs).

A criação de regras personalizadas para detecção e bloqueio de comportamentos específicos é um requisito. Abrangência e compatibilidade de ambiente

A solução deve implementar proteção contra ransomware que visa sistemas de armazenamento em rede (NAS, compartilhamentos SMB, etc.). Além disso, deve oferecer proteção para ambientes virtualizados e infraestruturas de desktop virtual (VDI). A implementação de mecanismos de detecção de anomalias baseados em linha de base comportamental do ambiente é crucial.

A compatibilidade com os principais sistemas operacionais do ambiente é essencial, incluindo:

· Windows: 10, 11, Server 2016, 2019, 2022.

· Linux: principais distribuições enterprise.

· macOS: as três versões mais recentes.

A solução deve implementar proteção contra ataques de ransomware direcionados a ambientes de nuvem e serviços SaaS.

Gerenciamento, integração e usabilidade

A solução deve oferecer dashboards personalizáveis com métricas de segurança, tentativas de ataques bloqueados e status de proteção dos endpoints. A geração de relatórios detalhados sobre tentativas de ataques e a eficácia das proteções implementadas é um requisito.

Para a administração, deve implementar controle de acesso baseado em funções (RBAC). A solução precisa oferecer capacidade de operação offline, mantendo proteções ativas mesmo quando o endpoint estiver desconectado. A integração nativa com soluções SIEM, EDR e SOAR para correlacionamento de eventos e resposta a incidentes é fundamental.

A solução deve oferecer proteção contra modificações não autorizadas de suas configurações e componentes e permitir a implementação de políticas baseadas em localização geográfica e contexto de rede (corporativa, pública, VPN).

Por fim, a solução deve oferecer um console de gerenciamento centralizado com capacidade de administração baseada em web. Deve ter capacidade de integração com ferramentas de backup e recuperação para orquestração da resposta a incidentes e permitir a exportação de dados em formatos padrão (CSV, JSON, PDF) para integração com ferramentas de análise externas.

ITEM 2.5 Requisitos Funcionais da Solução de *Threat Intelligence*

A solução de Threat Intelligence é um componente estratégico para prover inteligência acionável, aprimorando as capacidades preventivas e reativas de segurança.

Coleta e normalização de dados

A solução deve possuir mecanismos de coleta automatizada em múltiplas fontes OSINT (páginas web, redes sociais, fóruns especializados, aplicativos de mensageria, deep e dark web), com capacidade de extração contextual e semântica de conteúdos relevantes. Deverá conter um sistema de monitoramento de vazamentos relacionados a Marcas e VIPs, incluindo detecção precoce de campanhas, tentativas de

engenharia social e exposição não autorizada de informações sensíveis.

O mecanismo de normalização e indexação deve utilizar técnicas de processamento de linguagem natural (NLP) e análise semântica para pesquisa e análise eficiente em grandes volumes de dados heterogêneos. Um framework de integração extensível com múltiplas fontes de dados, incluindo feeds comerciais e comunitários de inteligência de ameaças de terceiros, com suporte a formatos padronizados (STIX/TAXII, MISP, OpenIOC), é fundamental.

Processamento e análise de ameaças

A solução precisa permitir a identificação e mapeamento de TTPs (Táticas, Técnicas e Procedimentos) baseados no framework MITRE ATT&CK, com correlação automática entre técnicas observadas e grupos de ameaças conhecidos (APTs). Um sistema avançado de classificação de ameaças que utilize modelos de inteligência artificial e machine learning, com capacidade de aprendizado contínuo e adaptação a novos padrões de ataque, é um requisito chave.

Deve possuir um mecanismo multidimensional de pontuação de risco baseado em heurísticas contextuais, Indicadores de Comprometimento (IoCs), relevância histórica e impacto potencial no ambiente específico da organização. A capacidade de identificação, correlação e atribuição de ameaças em tempo real, com análise comportamental para detecção de anomalias e atividades maliciosas emergentes, é essencial.

A plataforma deve incluir orquestração e automação no processo de coleta, análise e resposta a incidentes, com workflows personalizáveis e integração com sistemas de ticketing e SOAR (Security Orchestration, Automation and Response).

Monitoramento contínuo e resposta a incidentes

A solução deve suportar a implementação de honeynets distribuídas e adaptativas para detecção proativa de comportamento adversário, com emulação de ambientes corporativos realistas e capacidade de fingerprinting de atacantes. Um sistema de alertas em tempo real com múltiplos canais de notificação para detecção de ataques cibernéticos direcionados, incluindo mecanismos de priorização baseados em criticidade e contexto organizacional, é crucial.

Será necessário contar com uma solução de detecção e prevenção de vazamentos de credenciais e informações sensíveis, com monitoramento contínuo de credenciais comprometidas em bases de dados públicas e privadas. O monitoramento especializado e contextualizado de campanhas de phishing, ameaças persistentes avançadas (APT), ransomware-as-a-service e vazamentos de dados, com capacidade de análise forense e reconstrução de eventos, é um requisito. A solução deve apresentar uma arquitetura escalável e distribuída para atender diferentes volumes de dados e necessidades operacionais, com capacidade de processamento elástico e balanceamento dinâmico de carga.

Painel de controle e relatórios estratégicos

Para a visualização e gestão, a solução deve oferecer uma interface gráfica intuitiva e responsiva para gestão e análise de ameaças, com visualizações interativas para investigações detalhadas. Dashboards personalizáveis com métricas de risco, tendências de ataques e indicadores-chave de desempenho (KPIs) de segurança, adaptáveis a diferentes perfis de usuários e níveis organizacionais, são fundamentais.

A solução deve permitir a geração automatizada de relatórios técnicos detalhados para auditoria e conformidade, incluindo trilhas de evidências, análise de impacto e recomendações de mitigação. Um sistema avançado de exportação de relatórios customizados em múltiplos formatos (PDF, HTML, JSON, CSV) para auditorias, tomada de decisão estratégica e compartilhamento seguro com stakeholders é essencial. Além disso, um módulo de inteligência executiva com síntese de ameaças relevantes e tendências emergentes, traduzindo dados técnicos em insights acionáveis para a alta administração, é um diferencial.

Integração e interoperabilidade

A solução de Threat Intelligence deve possuir capacidade nativa de integração bidirecional com soluções de segurança existentes, incluindo SIEM, EDR, NDR, firewalls e sistemas de proteção de endpoints. A disponibilização de APIs RESTful documentadas e SDKs para desenvolvimento de integrações

customizadas e extensões da plataforma é um requisito.

O suporte a padrões abertos de compartilhamento de inteligência de ameaças (STIX/TAXII 2.1, OpenIOC, MISP) para interoperabilidade com ecossistemas externos é crucial. Por fim, a solução deve oferecer mecanismos seguros de compartilhamento seletivo de indicadores e inteligência com parceiros e comunidades de confiança, com controles granulares de acesso e anonimização quando necessário.

Gestão de conhecimento e colaboração

A solução deve prover uma base de conhecimento centralizada e pesquisável de ameaças, vulnerabilidades e procedimentos de resposta, com capacidade de versionamento e controle de acesso baseado em papéis. Deverá conter ferramentas colaborativas integradas para análise conjunta de ameaças, incluindo anotações compartilhadas, espaços de trabalho virtuais e fluxos de aprovação.

Um sistema de gestão de casos para coordenação de investigações complexas, com atribuição de tarefas, acompanhamento de progresso e documentação estruturada, é necessário. Por fim, a solução deve possuir mecanismos de feedback e aprendizado contínuo para refinamento de regras de detecção e modelos analíticos com base em resultados operacionais.

ITEM 2.6 Requisitos Minimos da Solução CSPM

A solução WAF deve oferecer proteção em tempo real para aplicações web, APIs e aplicativos móveis contra uma ampla gama de ameaças cibernéticas. Deverá permitir modos de detecção e bloqueio (por regra ou global), criação de regras com expressões regulares e parâmetros diversos (tamanho, conteúdo etc.), aplicação de novas regras sem impacto em sessões ativas e personalização da resposta de bloqueio, inclusive com HTML customizado. A solução deve suportar políticas granulares por aplicação, controle de métodos HTTP e cabeçalhos, listas de IPs (whitelist/blacklist) com liberação temporária ou permanente, e exceções por assinatura ou regra (ajuste fino).

Também deverá detectar e bloquear ataques como SQL Injection, XSS, CSRF, Command Injection, sequestro de sessão, entre outros. A proteção deve se estender a APIs REST/JSON, com parsing avançado. A plataforma deve implementar machine learning para modelagem de comportamento e criação automatizada de políticas, além de permitir a geração de relatórios customizáveis com agendamento, envio por e-mail e exportação em HTML e PDF.

ITEM 2.7 Requisitos Minimos da Solução WAF

A solução CSPM deve realizar análise contínua e automatizada da postura de segurança em ambientes de nuvem, detectando alterações em tempo real e identificando configurações inseguras em recursos de computação, redes, storage e gerenciamento de identidades. Deve validar conformidade com benchmarks reconhecidos (como CIS e NIST) e normas regulatórias (LGPD, PCI-DSS, ISO 27001, entre outras), além de oferecer templates e regras personalizáveis. A solução deve manter inventário atualizado dos recursos cloud monitorados, identificar exposições indevidas (como buckets públicos), fornecer descrições e recomendações de correção, e suportar políticas de auto- remediação. Também deverá analisar templates de IaC (CloudFormation, Terraform) e integrar-se com pipelines de CI/CD, ferramentas de automação,

sistemas de ticketing (como Jira, ServiceNow) e plataformas de colaboração (como Teams, Slack). Deve permitir exportação de relatórios por conta, grupo ou região, operar com privilégios mínimos e oferecer autenticação forte e controle de acesso baseado em funções (RBAC).

ITEM 2.8 Requisitos Minimos da Solução Pentest

A solução de Pentest deverá realizar simulações controladas de ataques cibernéticos com o objetivo de identificar vulnerabilidades técnicas e lógicas nos sistemas, aplicações, redes e infraestrutura em nuvem dos órgãos e entidades. Os testes deverão utilizar metodologias amplamente reconhecidas (como OWASP, NIST ou PTES), podendo ser realizados em diferentes níveis de acesso (caixa preta, cinza e branca), e contemplar tanto ameaças externas quanto internas. A solução deverá gerar relatórios técnicos e executivos contendo evidências, análise de risco, recomendações de mitigação e validação da eficácia dos controles de segurança existentes (como EDR, SIEM, WAF e SOAR). O serviço deverá prever a realização periódica de testes e permitir a execução de retestes para validação de correções, bem como apoiar os órgãos na priorização das falhas encontradas e na resposta a incidentes identificados durante os testes.

ITEM 2.9 Requisitos de Instalação e Configuração

Esta seção detalha os requisitos para a instalação e configuração das soluções de segurança, garantindo sua plena operacionalidade e integração no ambiente do CONTRATANTE.

A equipe responsável deverá realizar a instalação da solução de SIEM necessária para a operação do Centro de Operações de Segurança - Monitoramento de Incidentes Cibernéticos. Isso inclui a integração das fontes de Logs na solução de SIEM e a integração da solução de SIEM com a ferramenta de ITSM (ServiceNow).

Será fundamental integrar ferramentas de proteção de e-mail e antispam com soluções SIEM para correlacionar eventos relacionados a comportamentos anômalos observados em campanhas de phishing, automatizar a resposta a e-mails maliciosos (como exclusão ou quarentena em massa), e fornecer relatórios centralizados e métricas específicas sobre e-mails de alto risco.

A implementação de fluxos de trabalho automatizados para otimizar a triagem e resposta a incidentes é um requisito chave, abrangendo ações como contenção de ameaças, bloqueio de endereços IP ou domínios maliciosos, e integração com ferramentas de proteção como XDR e firewalls.

A equipe deverá propor a criação, alteração, customização, renomeação e/ou exclusão de regras de correlação baseadas em descobertas e análises de novas ameaças (IoCs e TTPs), redução na taxa de falsos positivos e eventos não relevantes, e melhoria da detecção de incidentes críticos com base nos cenários de uso mais relevantes para o contratante.

A automação de workflows de resolução de alertas e incidentes será realizada em colaboração sempre que aplicável, integrando ações como contenção de ameaças, bloqueio de endereços IP ou domínios baseados em políticas, e integração com ferramentas de resposta como EDR e XDR.

Serão propostas melhorias contínuas nos fluxos de trabalho do SIEM e SOAR, incluindo ajustes em regras de correlação para maior precisão, integração com novas fontes de dados e inteligência de ameaças, e redução do tempo médio de resposta (MTTR) por meio de automação e orquestração. Finalmente, será crucial garantir a integração contínua entre SIEM, SOAR e outras ferramentas de segurança, como XDR, para melhorar a visibilidade e a eficiência na detecção e resposta a incidentes.

ITEM 3. Requisitos do Serviço Pontual de Resposta a Incidentes ITEM 3.1 Atendimento Nível 1 (N1)

O Atendimento Nível 1 (N1) constitui a linha de frente operacional do SOC (Security Operations Center), responsável pela triagem qualificada e resposta inicial a eventos no ambiente tecnológico governamental. Este nível de serviço tem como objetivo principal garantir a detecção precoce, categorização precisa e contenção imediata de incidentes de segurança cibernética, operando como o primeiro filtro de defesa e um elemento crítico na redução do tempo médio de detecção (MTTD) e resposta (MTTR) a ameaças.

Escopo do Serviço de Atendimento N1 de SOC

O escopo do serviço de atendimento N1 do SOC deverá abranger as seguintes atividades e capacidades:

- Monitoramento Contínuo e Proativo

A equipe de N1 será responsável pela análise de alertas e eventos de segurança gerados por múltiplas fontes, incluindo SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), NDR (Network Detection and Response), sistemas de proteção de perímetro, sistemas de autenticação e soluções de segurança em nuvem implementadas na infraestrutura do órgão. Realizará o correlacionamento avançado de eventos utilizando técnicas de análise comportamental e contextual para identificação de padrões de ataque, anomalias e ameaças potenciais, visando reduzir falsos positivos e priorizar alertas genuínos. É essencial o registro detalhado e a categorização sistemática de eventos suspeitos com base em matriz de criticidade, considerando impacto potencial, superfície de ataque afetada, sensibilidade dos ativos envolvidos e contexto operacional. Além disso, haverá o monitoramento proativo de indicadores de comprometimento (IoCs) e inteligência de ameaças aplicável ao ambiente governamental, antecipando-se a possíveis vetores de ataque direcionados.

- Triagem e Análise Qualificada

O N1 fará a classificação de incidentes de segurança com base em critérios objetivos de impacto, urgência, propagação potencial e relevância para ativos críticos, utilizando metodologias reconhecidas como CVSS (Common Vulnerability Scoring System) adaptadas ao contexto governamental. Será aplicada sistematicamente a execução de playbooks e procedimentos padronizados para investigação inicial e tratamento de eventos, garantindo consistência operacional e conformidade com as melhores práticas de resposta a incidentes. Um sistema estruturado de notificações e alertas aos responsáveis será acionado conforme matriz de escalonamento predefinida, com múltiplos canais de comunicação e confirmação de recebimento. Toda a documentação forense e o registro cronológico detalhado das atividades serão mantidos no sistema de ITSM (Information Technology Service Management) ou plataforma equivalente, preservando evidências e garantindo rastreabilidade completa das ações executadas.

- Resposta Inicial a Incidentes

A equipe de N1 deverá realizar a implementação imediata de medidas de contenção e mitigação conforme definido nas diretrizes e playbooks de resposta a incidentes, incluindo isolamento de sistemas comprometidos, bloqueio de tráfego malicioso e revogação temporária de credenciais suspeitas. Fará a execução coordenada de ações corretivas pré-autorizadas para incidentes de baixa e média criticidade, seguindo procedimentos documentados e aprovados pela governança de segurança do órgão. Um mecanismo estruturado de escalonamento para o nível 2 (N2) será acionado em casos que demandem análise forense aprofundada, resposta especializada ou ações que excedam o escopo de autorização do N1, com transferência documentada de contexto e evidências. Além disso, será mantida uma comunicação proativa e transparente com equipes internas, gestores de TI e partes interessadas para atualização do status do incidente, seguindo protocolos de comunicação predefinidos e adequados ao nível de criticidade.

- Relatórios e Indicadores de Desempenho

O N1 será responsável pela geração automatizada de relatórios periódicos (semanais e mensais) sobre os eventos de segurança

detectados, incluindo análises de tendências, categorização de incidentes, tempo médio de detecção e resposta, e eficácia das ações de contenção. Um dashboard em tempo real com métricas e indicadores-chave de desempenho (KPIs) para avaliação contínua da eficiência do atendimento N1 será mantido, incluindo volume de alertas processados, taxa de falsos positivos, tempo médio de triagem e percentual de resolução no primeiro nível. Haverá também análise retrospectiva de incidentes com identificação de padrões recorrentes, pontos de melhoria nos processos de detecção e oportunidades de refinamento nas regras de correlação e playbooks de resposta. Por fim, serão produzidos relatórios executivos customizados para diferentes níveis hierárquicos, traduzindo dados técnicos em informações acionáveis para tomada de decisão estratégica.

- Melhoria Contínua e Gestão do Conhecimento

Para a melhoria contínua, ocorrerá a revisão periódica e atualização dos procedimentos operacionais com base em lições aprendidas, novas ameaças identificadas e evolução das táticas, técnicas e procedimentos (TTPs) dos adversários. Será mantida uma base de conhecimento estruturada com histórico de incidentes, soluções aplicadas e procedimentos de mitigação, acessível à equipe de segurança para referência rápida em situações similares. A equipe terá participação ativa em exercícios de simulação de incidentes e testes de resposta, contribuindo para o refinamento contínuo dos processos de detecção e resposta. Haverá compartilhamento controlado de informações sobre ameaças com a comunidade de segurança governamental, respeitando políticas de confidencialidade e classificação de informações.

- Requisitos Técnicos e Operacionais do N1

O serviço de N1 deve garantir disponibilidade ininterrupta (24x7x365), com equipe especializada dimensionada adequadamente para cobertura contínua sem degradação da qualidade do atendimento, incluindo planos de contingência para situações de crise. É fundamental a conformidade comprovada com normas e frameworks de segurança reconhecidos internacionalmente, como ISO/IEC 27001:2022, NIST SP 800-61r2 (Computer Security Incident Handling Guide), NIST Cybersecurity Framework e requisitos específicos da Lei Geral de Proteção de Dados (LGPD). A infraestrutura de comunicação deve ser redundante para garantir a continuidade operacional mesmo em cenários de degradação de conectividade, incluindo canais alternativos para notificação de incidentes críticos. Por fim, o ambiente de operação da equipe N1 deve ser seguro e controlado, com controles de acesso físico e lógico, monitoramento ambiental e conformidade com requisitos de segurança física para centros de operação críticos.

ITEM 3.2 Atendimento Nível 2 (N2)

O Atendimento Nível 2 (N2) constitui a camada especializada de análise e resposta do SOC, responsável pela investigação aprofundada, contenção avançada e remediação efetiva de incidentes de segurança cibernética que excedem o escopo de resolução do Nível 1. Esta equipe atua como o núcleo técnico-analítico do SOC, empregando metodologias forenses, técnicas avançadas de hunting e conhecimento especializado em vetores de ataque para identificar, neutralizar e erradicar ameaças que comprometam ou possam comprometer a integridade, confidencialidade e disponibilidade dos ativos informacionais do ambiente governamental.

Escopo do Serviço de Atendimento N2 de SOC

O escopo do serviço de atendimento N2 do SOC deverá abranger as seguintes atividades e capacidades: - Análise Avançada de Incidentes e Investigação Forense

A equipe de N2 realizará a investigação forense aprofundada de eventos e incidentes de segurança escalonados pelo N1, utilizando metodologias estruturadas e ferramentas especializadas para reconstrução cronológica e análise de evidências digitais. Será feita a aplicação de técnicas avançadas de digital forensics e incident response (DFIR), incluindo análise de memória volátil, exame de artefatos do sistema operacional, inspeção de tráfego de rede criptografado e análise comportamental de malware. É essencial a identificação e caracterização de táticas, técnicas e procedimentos (TTPs) utilizados por atores maliciosos, com mapeamento para frameworks como MITRE ATT&CK e Diamond Model of Intrusion Analysis. Haverá a utilização de plataformas de threat intelligence para enriquecimento contextual das análises, correlacionando indicadores técnicos com informações sobre grupos de ameaças, campanhas conhecidas e motivações de atacantes. Por fim, será conduzida a análise de causa-raiz para determinar vetores iniciais de comprometimento, falhas de controle exploradas e extensão completa do impacto em incidentes confirmados.

- Contenção e Remediação Especializada

O N2 será responsável pelo desenvolvimento e implementação de estratégias de contenção customizadas para limitar

o impacto e propagação de incidentes confirmados, considerando criticidade dos ativos, janelas operacionais e potenciais efeitos colaterais. Haverá coordenação técnica com equipes de TI, segurança e áreas de negócio para execução sincronizada de ações de contenção e remediação, garantindo alinhamento com processos de gestão

de mudanças e continuidade de negócios. A implementação de regras de detecção e bloqueio em múltiplas camadas de segurança (EDR, NDR, SIEM, firewalls, proxy, AntiSpam) será baseada em indicadores técnicos e comportamentais identificados durante a investigação. Também será realizado o desenvolvimento de scripts e automações personalizadas para resposta a incidentes específicos, acelerando a contenção e remediação em larga escala quando necessário. Por fim, serão conduzidas varreduras especializadas para identificação de persistência, movimentação lateral e backdoors instalados por atacantes, garantindo erradicação completa da ameaça.

- Threat Hunting e Detecção Proativa

A equipe de N2 realizará operações regulares de threat hunting baseadas em hipóteses, utilizando técnicas avançadas de busca e correlação para identificar ameaças que tenham evadido os mecanismos de detecção automatizados. Haverá desenvolvimento e refinamento contínuo de regras de correlação avançadas em plataformas SIEM, para detecção de padrões complexos de ataque. Será feita a identificação proativa de comportamentos anômalos e suspeitos através de análise estatística, machine learning e modelagem de comportamento de usuários, entidades e redes (UEBA). A equipe realizará a integração e operacionalização de feeds de threat intelligence para detecção antecipada de campanhas emergentes e ameaças direcionadas ao setor governamental. Além disso, serão realizadas análises de vulnerabilidade contextualizadas em ativos críticos, correlacionando exposições técnicas com ameaças ativas e capacidades de exploração conhecidas.

- Gestão Avançada de Incidentes

O N2 será responsável pela classificação e priorização dinâmica de incidentes críticos com base em impacto operacional, sensibilidade dos dados afetados, propagação potencial e alinhamento com objetivos estratégicos da organização. Haverá coordenação de comunicação técnica e executiva durante incidentes de alta criticidade, incluindo preparação de briefings situacionais, recomendações táticas e atualizações de status para diferentes níveis hierárquicos. A equipe fará a liderança técnica em células de crise (war rooms) para resposta coordenada a incidentes complexos, garantindo sincronização entre equipes técnicas, jurídicas, de comunicação e alta administração. A documentação forense detalhada e juridicamente defensável de todas as atividades, evidências e ações tomadas será mantida, preservando cadeia de custódia e garantindo conformidade com requisitos legais e regulatórios. Por fim, serão conduzidas análises pós-incidente (lições aprendidas) para identificação de oportunidades de melhoria nos controles de segurança, processos de detecção e procedimentos de resposta.

- Inteligência e Análise Estratégica

A equipe de N2 será responsável pela elaboração de relatórios técnicos aprofundados sobre incidentes tratados pelo N2, incluindo análise forense, timeline de eventos, técnicas utilizadas pelo atacante e recomendações específicas de hardening. Deverá haver o desenvolvimento de análises de tendências de ameaças relevantes para o ambiente governamental, identificando padrões, setores mais visados e evolução de táticas adversárias. Por fim, será feita a produção de relatórios de inteligência acionável com recomendações preventivas baseadas em análise de campanhas recentes, vulnerabilidades zero-day e mudanças no panorama de ameaças.

- Requisitos Técnicos e Operacionais do N2

A equipe de N2 deve garantir disponibilidade ininterrupta do serviço (24x7x365), com equipe especializada dimensionada para capacidade de resposta simultânea a múltiplos incidentes complexos, incluindo esquemas de sobreaviso para especialistas em áreas específicas. Será necessária uma plataforma integrada de análise forense e resposta a incidentes com capacidade para processamento de grandes volumes de dados, análise de memória volátil, exame de artefatos de sistema e reconstrução de eventos de segurança. Um arsenal avançado de ferramentas especializadas é fundamental, incluindo soluções de threat intelligence, análise de malware (estática e dinâmica), forensics de rede, análise de logs, SIEM, EDR, NDR, SOAR e plataformas de orquestração de resposta. A equipe deverá operar em um ambiente seguro de análise de malware (sandbox) com capacidade de detonação controlada, engenharia reversa e análise comportamental de códigos maliciosos, isolado da infraestrutura principal. Por fim, haverá integração com sistemas de gestão de vulnerabilidades, CMDB e ferramentas de gestão de ativos para contextualização rápida durante investigações e priorização baseada em criticidade.

ITEM 3.3 Serviços Especializados

Os serviços especializados serão acionados para eventos com nível de criticidade alto e crítico, após análise em primeiro nível pelo Centro de Operações de Segurança - Monitoramento de Incidentes Cibernéticos. Estes serviços atuarão, através de horas especializadas, por meio dos seguintes critérios: englobar ações reativas, com base em eventos ocorridos; realizar pontualmente as atividades sem características de atuação permanente ou contínua; e abordar incidentes complexos, apoiando o incidente em todo o seu ciclo de vida, desde o estabelecimento até a resolução.

Um time de suporte avançado de resposta a incidentes será disponibilizado, e os serviços contemplados por este item são: coordenação da resposta avançada e contenção de incidentes de segurança; erradicação e recuperação; remediação de sistemas comprometidos; aplicação de patches e reconfiguração segura; restauração de backups seguros; e testes para garantir a eliminação da ameaça.

Será realizada a análise pós-incidente de causa raiz para a melhoria contínua dos processos e procedimentos e para gerar resiliência para a operação de segurança. Além disso, haverá a capacidade de identificar riscos potenciais por meio de análise de risco e se preparar para garantir que as tecnologias de monitoramento estejam devidamente configuradas para os incidentes de segurança.

Investigação Forense Digital

No âmbito dos serviços especializados, a investigação forense digital abrangerá: coleta e preservação de evidências digitais; análise de memória, discos e artefatos do sistema operacional; engenharia reversa de malware; e análise de logs e correlação de eventos.

ITEM 4. Requisitos dos Serviços de Fornecimento das Salas de Monitoramento

Deverão ser disponibilizadas duas Salas de Monitoramento de Segurança da Informação, sendo uma nas dependências da SGGD (Sala I - SGGD) e outra nas dependências da CONTRATADA (Sala II - CONTRATADA), com a finalidade de prover infraestrutura física, computacional, de telecomunicações e operacional para viabilizar o monitoramento e a análise contínua de ameaças, bem como para apoiar ações de prevenção e mitigação de incidentes de cibersegurança no âmbito da SGGD.

A Sala I – SGGD deverá ser instalada em espaço a ser definido pela própria Secretaria. A Sala II – CONTRATADA deverá ser implantada em dependências próprias da CONTRATADA, devendo possuir configurações e características técnicas iguais ou superiores às da Sala I – SGGD. Caso a CONTRATADA já disponha, em data anterior à publicação deste Termo de Referência, de estrutura de Sala de Monitoramento de Segurança da Informação instalada e em operação em suas dependências, esta poderá ser utilizada para atender ao item “Sala II – CONTRATADA”, desde que atenda integralmente a todos os requisitos e exigências estabelecidos neste Termo de Referência.

A montagem física de ambas as Salas de Monitoramento de Segurança da Informação deverá ser concluída conforme o cronograma de execução contratual, contados a partir da assinatura do contrato, e ocorrer de forma concomitante à liberação do espaço físico a ser cedido pela SGGD, observadas as condições e os pré-requisitos operacionais detalhados nos tópicos seguintes.

A fase inicial de operação das Salas de Monitoramento de Segurança da Informação estará definida no Cronograma de Execução Contratual. Ambas as salas, Sala I – SGGD e Sala II – CONTRATADA, deverão possuir certificação ISO/IEC 27001 e classificação Triple AAA.

A CONTRATADA deverá utilizar, nas instalações da SGGD, as soluções e a infraestrutura fornecidas pela Secretaria, conforme descrito a seguir, com o

objetivo de assegurar: (i) o monitoramento e o tratamento de incidentes de segurança; e (ii) o registro, acompanhamento e análise de tickets, por meio das ferramentas e recursos disponibilizados pela SGGD, garantindo a rastreabilidade e a precisão das informações registradas.

Caberá à CONTRATADA realizar a manutenção dos equipamentos e bens fornecidos para a execução dos serviços, assegurando sua plena funcionalidade, inclusive providenciando, sempre que necessário, a substituição ou retirada daqueles que apresentarem defeitos.

A CONTRATADA será responsável pela desmontagem da Sala de Monitoramento de Segurança da Informação, Sala I – SGGD, sob sua exclusiva responsabilidade e sem quaisquer ônus a SGGD, e se obriga a providenciar a desinstalação e remoção de todos os equipamentos e bens disponibilizados no prazo máximo de 30 (trinta) dias corridos, contados a partir da data de formalização do pedido do CONTRATANTE.

· A utilização dos equipamentos e bens no período compreendido entre o encerramento do contrato e a remoção dos mesmos, não implicará em quaisquer custos adicionais ou pagamentos pela SGGD.

· Todos os equipamentos e bens de propriedade da CONTRATADA, deverão possuir etiqueta de identificação com suas informações básica, com razão social, Nome fantasia e Logomarca.

A SGGD deverá ressarcir a CONTRATADA por danos causados aos seus equipamentos e materiais nas seguintes situações:

· Defeitos, falhas ou danos ocasionados por problema na infraestrutura predial ou na rede elétrica ou lógica, ou por estas estarem fora dos padrões estabelecidos, desde que a CONTRATADA apresente laudo técnico específico;

· Defeitos, falhas ou danos ocasionados por vandalismo, assim consideradas aquelas situações em que ocorre depredação do equipamento, danificando-o no todo ou em parte, seja na alteração da configuração original do equipamento, mau uso ou queda, desde que causados por empregado do CONTRATANTE;

· Extravios, furtos ou roubos realizados após o recebimento dos equipamentos nas dependências do CONTRATANTE.

A CONTRATADA será responsável por prover, instalar, operar e manter todos os equipamentos e espaços necessários para a prestação do

serviço nas instalações da SGGD, incluindo, mas não se limitando a: Servidores Operacionais; Armazenamento Dedicado; Conectividade e acessórios (firewalls, switches, etc.); outros recursos necessários para atender às demandas contratuais, em completa compatibilidade com a infraestrutura já existente na SGGD.

A CONTRATADA será integralmente responsável pelo fornecimento, montagem, instalação e operação:

· Dimensões mínimas para as salas: Sala do videowall, devendo possuir dimensões mínimas de 6m x 4m (24m²), garantindo espaço adequado para a instalação de equipamentos, monitores, servidores e posicionamento de operadores e mobiliário; Sala de crise: Deve possuir dimensões mínimas de 5m x 5m (25m²), com áreas dedicadas para a tela principal, mesas de reunião e instalações complementares.

· Serviços de infraestrutura complementar, como: preparação das paredes e suportes para instalação das telas, assegurando solidez e adequação técnica; Elementos básicos de mobiliário, como mesas e cadeiras para operação e reuniões, compatíveis com o ambiente projetado.

· Dos equipamentos, incluindo: Um videowall composto por 6 telas de 55" com tecnologia LED ou LCD, para ambiente de monitoramento contínuo, que deverá atender aos seguintes requisitos: Resolução mínima de 4K Ultra HD (3840x2160 pixels), garantindo visualização precisa e detalhada dos múltiplos fluxos de informações; Suporte para montagem em mosaico/grade, permitindo exibição simultânea de dashboards, alertas e relatórios; Compatibilidade plena com ferramentas de monitoramento e resposta a incidentes, com conectividade para entradas HDMI, DisplayPort ou outros padrões de mercado; Estrutura física e elétrica adequada às instalações da SGGD, incluindo redundância de energia para operação ininterrupta.

· Uma sala de crise equipada com uma tela de 100" com tecnologia LED ou LCD, que deverá atender aos seguintes requisitos: Resolução mínima de 4K Ultra HD (3840x2160 pixels) para apresentação de informações estratégicas; Total conectividade com os sistemas instalados no Centro de Operações de Segurança - Monitoramento de Incidentes Cibernético da SGGD, incluindo integração com ferramentas de comunicação e videoconferência; Compatibilidade com múltiplos modos de apresentação, como dispositivos móveis e serviços multimídia; Suporte para infraestrutura de áudio e vídeo de alta qualidade compatível com a SGGD.

· Todos os equipamentos fornecidos e instalados pela CONTRATADA deverão seguir os seguintes requisitos técnicos e operacionais: Certificação de Tecnologia: Utilizar equipamentos certificados e compatíveis com normas internacionais de qualidade (ex.: ISO 9001) e eficiência energética; Testes de Compatibilidade: Garantir integração total e comprovada entre os equipamentos fornecidos e os sistemas existentes da SGGD; Documentação Técnica: Documentar todos os detalhes técnicos dos equipamentos instalados (modelos, especificações, planos de manutenção).

A CONTRATADA deverá cumprir todos os padrões de segurança e as regras de controle de acesso definidas pela SGGD, assegurando: rigoroso controle no acesso físico e lógico às salas onde os equipamentos serão instalados; Alinhamento às políticas de segurança da informação vigentes (como ISO/IEC 27001 ou equivalentes); Auditorias regulares para validar práticas seguras e eficazes de manutenção dos sistemas.

· Todo o suporte e manutenção preventiva dos equipamentos fornecidos ficará sob responsabilidade da CONTRATADA, incluindo: Inspeções técnicas regulares para prever e corrigir possíveis falhas nos equipamentos instalados; Garantia de funcionalidade contínua mediante substituição imediata de peças ou componentes defeituosos; Atualizações de software e firmware, conforme necessário, durante o período contratual.

· Toda a infraestrutura contratada deverá estar disponível 24x7x365, garantindo: Alta disponibilidade operacional de todos os equipamentos fornecidos; Recursos redundantes para prevenir qualquer falha de operação durante os serviços.

Responsabilidade da Contratante[JZ2]

Será de responsabilidade da SGGD, para a Sala I - SGGD, providenciar previamente e manter a seguinte infraestrutura, necessária à montagem da Sala de Monitoramento de Segurança da Informação, caso o local seja diferente do definido para a Sala II – CONTRATADA:

- Infraestrutura Predial

A SGGD deverá providenciar obra civil, rede elétrica estabilizada, cabeamento lógico estruturado, sistema de iluminação adequado, e solução de isolamento acústico. Além disso, é responsável por um gerador de energia para as áreas privativas, atendendo 100% da demanda, sistemas de nobreaks de alta performance para sustentar os equipamentos da sala, sistema de refrigeração de conforto central que atenda a sala ou equipamento similar, e solução de segurança e monitoramento do ambiente, incluindo controle de acesso e CFTV.

- Infraestrutura de TI

A SGGD deverá garantir uma rede segura, isolada e confiável para conectar todos os sistemas e dispositivos necessários, com sistema de suporte auxiliar de energia. A conexão segmentada da rede corporativa em alta disponibilidade deve ser alimentada por 02 (dois) provedores distintos de rede WAN, de forma que a falha de uma conexão isoladamente não afete o funcionamento da operação. Serão fornecidos firewalls, IDS/IPS (Intrusion Detection/Prevention Systems) e outras medidas de segurança para proteger a rede isolada já implementados, além dos servidores. Por fim, a SGGD deverá disponibilizar um link dedicado, com conexão segura ponta a ponta entre as Salas de Monitoramento de Segurança da Informação (Sala I – SGGD e Sala II – CONTRATADA), corretamente dimensionado em capacidade de acordo com as necessidades da execução dos serviços a serem prestados.

- Requisitos de Segurança de TI

A CONTRATADA será responsável por garantir a disponibilidade, confidencialidade e integridade de todas as atividades desempenhadas, bem como das informações processadas, armazenadas e transmitidas, utilizando práticas e tecnologias adequadas para proteção de dados contra acessos não autorizados, perdas ou alterações.

A CONTRATADA deverá garantir o cumprimento do critério de menor privilégio nas configurações de firewalls, roteadores e demais periféricos de camadas de rede, minimizando os níveis de acesso fornecidos e restringindo permissões desnecessárias, de modo a mitigar potenciais vulnerabilidades.

A CONTRATADA deverá garantir segurança em qualquer solução de sua propriedade que venha a utilizar os recursos tecnológicos da SGGD, adotando medidas como: Avaliações de conformidade e segurança para soluções implementadas; Monitoramento constante para identificar e mitigar ameaças; Adoção de processos alinhados às normas ISO/IEC 27001 ou equivalentes, além de boas práticas de mercado para proteção de dados.

- Requisitos de Segurança Física

A CONTRATADA deverá implementar rigorosos sistemas de controle de acesso físico, garantindo que apenas usuários ou terceiros devidamente autorizados possam entrar nas áreas destinadas ao processamento, armazenamento e monitoramento das atividades desempenhadas. Esses controles deverão incluir, no mínimo: Identificação e autenticação para entrada nas áreas restringidas; Registro de acessos realizados, mantendo logs atualizados e seguros, disponíveis para auditorias ou consultas a qualquer momento.

A CONTRATADA deverá implementar sistemas de detecção de intrusões e alarmes em tempo real para proteger os ambientes onde serão

desempenhadas as atividades de monitoramento de incidentes, assegurando resposta imediata a tentativas de acessos não autorizados.

A CONTRATADA deverá implementar e manter sistemas de prevenção e combate a incêndios, de acordo com normas técnicas nacionais vigentes (ex.: ABNT NBR 17240) e com as melhores práticas de proteção. Esses sistemas deverão englobar, no mínimo: Hidrantes, extintores e sistemas de sprinklers; sensores de detecção de fumaça e calor; Medidas de evacuação de ambientes em caso de emergência; Inspeções e manutenções regulares para assegurar a plena funcionalidade dos sistemas.

A CONTRATADA deverá instalar e manter em funcionamento câmeras de monitoramento de segurança nos ambientes em que serão desempenhadas as atividades contratadas, garantindo que: As imagens captadas pelas câmeras sejam armazenadas com segurança por um período definido no contrato, assegurando acesso aos registros sempre que solicitado pela SGGD; os sistemas de vídeo vigilância sejam monitorados em tempo real para pronta resposta em caso de ocorrências.

7. REQUISITOS NÃO FUNCIONAIS

O ambiente tecnológico da SGGD e demais órgãos contemplados nesse projeto, necessitam de monitoramento abrangente, incluindo todos os ativos e tecnologias atualmente em uso. A CONTRATADA será responsável por este monitoramento.

8. CLASSIFICAÇÃO DE SEVERIDADE DE INCIDENTES

Os eventos serão gerenciados ao longo do processo de monitoramento considerando sua urgência e impacto, além disso a criticidade inicialmente atribuída poderá ser reavaliada e ajustada, mediante justificativa adequada e aprovação da SGGD. A definição do grau de severidade será realizada com base nos seguintes critérios:

CARACTERÍSTICA DE GRAVIDADE
CRÍTICO: Falha que compromete significativamente o uso do sistema em um ambiente de produção, como a perda de dados operacionais ou a indisponibilidade total dos sistemas produtivos. Essa condição impede a continuidade das operações da empresa, sem possibilidade de solução alternativa por meio de procedimentos.
ALTA CRITICIDADE: Cenário em que o sistema permanece operante, porém com uma redução significativa na sua utilização em um ambiente de produção. Essa condição está gerando um impacto considerável em áreas críticas das operações da empresa, sem possibilidade de soluções alternativas por meio de procedimentos.
MÉDIA CRITICIDADE: Questão que resulta em uma perda parcial e não essencial na usabilidade do sistema, seja em um ambiente de produção ou de desenvolvimento. Em ambientes de produção, o impacto nos negócios é leve ou moderado, mas as operações seguem em funcionamento, inclusive com o uso de uma solução alternativa. Em ambientes de desenvolvimento, ocorre quando a situação leva à interrupção do projeto ou impede a migração para a produção.
BAIXA CRITICIDADE: Questão de interesse geral, relato de inconsistência na documentação ou sugestão de melhoria ou ajuste para um produto futuro. Em ambientes de produção, há pouco ou nenhum impacto nas operações do seu negócio, no desempenho ou na funcionalidade do sistema. Já em ambientes de desenvolvimento, o impacto nos negócios é leve ou moderado, mas as atividades continuam operando, incluindo a possibilidade de uso de uma solução alternativa por meio de procedimento.

Após identificar a gravidade do evento, deve-se desenvolver um procedimento de atendimento levando em conta os seguintes aspectos:

Classificação do Incidente	Prazo Máximo de Resposta	Prazo Máximo de Resolução	Procedimento Exigido
Crítico	30 minutos	Conforme plano de ação	· Registro imediato e notificação formal à SGGD. · Criação da Sala de Crise com especialistas; · Acionar a equipe de resposta pontual de incidentes ou especialistas integrados a SGGD. Nesse período, soluções temporárias podem ser aplicadas para mitigar impactos enquanto a resolução definitiva é executada. · Monitoramento contínuo até a resolução;
Alta Criticidade	45 minutos	4 horas	· Registro em sistema de controle de eventos; · Comunicação ativa com gestores da SGGD; · Acionar a equipe de resposta pontual de incidentes ou especialistas integrados a SGGD. Nesse período, soluções temporárias podem ser aplicadas para mitigar impactos enquanto a resolução definitiva é executada. · Monitoramento contínuo até a resolução;

Média Criticidade	1 hora	8 horas	· Registro em sistema de controle de eventos; · Comunicação ativa com gestores da SGGD; · Monitoramento contínuo até a resolução; · Inclusão no relatório periódico com as ações corretivas realizadas.
Baixa Criticidade	4 horas	48 horas	· Registro em sistema de controle de eventos; · Direcionamento aos técnicos responsáveis; · Tratamento pontual do evento, quando aplicável; · Inclusão no relatório periódico com as ações corretivas realizadas

9. PARCELAMENTO DA SOLUÇÃO DE TIC

O SOC constitui-se como uma estrutura integrada e especializada por lidar com tratamento de questões relacionadas à segurança da informação, não se caracterizando como uma unidade isolada. Entre suas funções típicas, destacam-se o Monitoramento e Gestão de Vulnerabilidades, Monitoramento Contínuo de Eventos de Segurança, Gestão da Resposta a Incidentes de Segurança, Gestão das Ameaças de Segurança, entre outras atividades correlatas.

Todas essas funções dependem da utilização de ferramentas tecnológicas e de recursos humanos qualificados para a configuração, análise e aplicação de inteligência sobre os eventos detectados ou identificados. Nesse sentido, se a responsabilidade pela configuração, análise e aplicação de inteligência recair integralmente sobre o SOC, poderá haver prejuízo na execução das atividades de monitoramento e gestão, considerando o elevado volume de informações que requerem tratamento em tempo real.

As ferramentas que automatizam os processos do SOC exigem ajustes contínuos em seus algoritmos e modelos de inteligência, demandando assim de uma equipe exclusivamente dedicada a esse propósito. Dessa forma, a infraestrutura do SOC (licenças e ambiente físico) e os serviços técnicos devem operar de forma sinérgica, porém com a adequada divisão de responsabilidade, o SOC voltado prioritariamente ao monitoramento e à gestão dos serviços de Segurança da Informação, e a equipe técnica dedicada às atividades de análise e inteligência.

A eficácia do monitoramento e da gestão depende diretamente da qualidade da análise e da aplicação de inteligência, sendo imprescindível que haja comunicação rápida, eficaz e sem entraves administrativos ou burocráticos, de modo a assegurar a resposta tempestiva e precisa aos incidentes de segurança da informação. Afinal, a capacidade de reação em tempo de resposta reduzido é essencial para mitigar os impactos decorrentes de eventos críticos.

Diante dessa necessidade de integração operacional, comunicação rápida e atuação coordenada, os itens que compõem a solução devem ser agrupados em um único lote, a ser provido por uma mesma empresa, garantindo a plena sinergia entre o ambiente físico do SOC e os serviços técnicos especializados.

Dessa forma, o parcelamento da solução ora CONTRATADA não se mostra tecnicamente viável, sendo juridicamente amparado e justificado sob a ótica da economicidade e da eficiência na gestão do contrato administrativo, em conformidade com o artigo 32, inciso II, da Lei Federal nº 13.303, de 30 de junho de 2016.

No presente caso, a fragmentação implicaria em maiores custos administrativos, dificultando assim a gestão integrada do contrato e comprometeria a eficiência, controle, cumprimento de prazos e a observância dos NMSE previstos, além de gerar a necessidade de duplicidade de esforções de fiscalização e gerenciamento.

A operacionalização e gestão da solução CONTRATADA devem ser centralizadas sob a responsabilidade de um único prestador de serviços, de modo a garantir a integração plena das atividades, a agilidade na comunicação, o atendimento rápido dos incidentes e a otimização dos recursos disponíveis.

Em suma, a opção pelo não parcelamento do objeto considera a necessidade de unificação da operacionalização e do gerenciamento da solução, assegurando a plena integração dos serviços, a otimização dos recursos disponíveis e a eficiência na gestão do contrato. Dessa forma, a contratação em um único lote encontra respaldo técnico e jurídico, de forma a estar alinhado aos princípios da economicidade e eficiência, sendo indispensável para a efetividade na implantação do SOC.

10. FORMA DE CONTRATAÇÃO E REGIME DE EXECUÇÃO

A contratação do objeto pretendido refere-se à prestação de serviços comuns de tecnologia da informação, sem o fornecimento de mão de obra em regime de dedicação exclusiva, a ser realizada mediante contratação direta, nos termos da Política de Aquisições para Operações Financiadas pelo Banco Interamericano de Desenvolvimento – BID (GN 2349-15).

O regime de execução do contrato será empreitada por preço unitário.

A escolha da PRODESP como entidade executora fundamenta-se em sua atribuição legal como prestadora de serviços de tecnologia da informação e comunicação para a Administração Pública Estadual, nos moldes de seu estatuto social. Nesse contexto, compete à PRODESP desenvolver, implementar, operar e manter soluções de TIC em benefício dos órgãos e entidades do Governo do Estado de São Paulo, sendo reconhecida como entidade estratégica para o atendimento das demandas de transformação digital e segurança da informação.

Nos termos do artigo 74, inciso III, da Lei Federal nº 14.133, de 1º de abril de 2021 (Nova Lei de Licitações e Contratos Administrativos), é permitida a contratação direta de empresa pública ou sociedade de economia mista que atue no âmbito da Administração Pública e cuja atividade principal seja compatível com o objeto contratado, dispensando-se a realização de procedimento licitatório tradicional.

A centralização da contratação por meio da Prodesp visa garantir maior eficiência, padronização, celeridade e economicidade no atendimento às demandas da SGGD, considerando que, conforme previsto no Contrato de Empréstimo BID 5579/OC-BR (BR-L1591), a medida possui respaldo técnico, uma vez que a Prodesp é responsável pelo suporte a infraestrutura tecnológica, bem como prover soluções tecnológicas e serviços técnicos relacionados à segurança cibernética da SGGD.

Ademais, a PRODESP já dispõe de infraestrutura tecnológica, capacidade técnica e experiência comprovada na operação de projetos de grande escala em segurança da informação, transformação digital e atendimento a políticas públicas de modernização da gestão, o que contribui para a redução de riscos e para o atendimento tempestivo das metas estabelecidas no Projeto São Paulo Mais Digital.

Por fim, a contratação da Prodesp está em consonância com as diretrizes da Estratégia de Governo Digital instituída pelo Decreto nº 67.799/2023, especialmente quanto ao art. 7º e parágrafo único, que estabelece:

> ***"Artigo 7° - A Companhia de Processamento de Dados do Estado de São Paulo - PRODESP tem por atribuição prestar, na forma de seu estatuto social, os serviços detecnologia da informação e comunicação necessários ao Sistema Estadual de Tecnologia da Informação - SETIC, de que trata o Decreto n° 64.601, de 22 denovembro de 2019, e à execução da Estratégia de Governo Digital e dos Planos Diretores de Tecnologia da Informação e Comunicação previstos neste decreto.***
>
> ***Parágrafo único - Cabe aos órgãos e entidades priorizar a contratação da PRODESP para prestação dos serviços de que trata o "caput" deste artigo, observadas as normas legais e regulamentares aplicáveis à espécie."***

11. DEFINIÇÃO DAS RESPONSABILIDADE DA SGGD E DA CONTRATADA

Para a prestação dos serviços, a CONTRATADA deverá disponibilizar as ferramentas de ITSM e demais aplicações de segurança necessárias para a execução do escopo definido. A gestão, manutenção e o controle de acesso a essas ferramentas serão de responsabilidade exclusiva da CONTRATADA.

A operação e uso das soluções e aplicações disponibilizadas deverão ocorrer por meio de VPN via internet ou link dedicado, cuja configuração, manutenção e pleno funcionamento ficarão sob a responsabilidade integral da CONTRATADA.

A infraestrutura tecnológica necessária à prestação dos serviços, compreendendo estações de trabalho, softwares necessários para a execução dos serviços pertinentes, bem como as conexões físicas e lógicas à rede da SGGD, deverá ser provida, gerida e mantida pela CONTRATADA.

Compete à CONTRATADA garantir a plena operacionalidade dos serviços no prazo estabelecido no cronograma de execução contratual, contados a partir da assinatura do contrato, podendo este prazo ser prorrogado a critério exclusivo da SGGD, ou mediante acordo formal entre as partes.

Todas as ferramentas e soluções de software disponibilizadas pela CONTRATADA devem estar plenamente compatíveis com as aplicações e tecnologias adotadas pela SGGD. Caso sejam constatadas incompatibilidades, compete à CONTRATADA realizar imediatamente as adequações necessárias, sem qualquer ônus adicional para a SGGD.

A SGGD, a seu exclusivo critério, poderá: atualizar as versões de sistemas operacionais, linguagens de desenvolvimento, ferramentas integrantes de sua plataforma tecnológica, modificar padrões, normas, processos e ferramentas de apoio adotadas no ambiente operacional. Cabe à CONTRATADA adaptar-se prontamente a tais atualizações, garantindo o uso contínuo de suas soluções sem comprometer os prazos ou a qualidade dos serviços prestados.

Todos os entregáveis produzidos durante a vigência do contrato serão de propriedade exclusiva da SGGD, que poderá utilizá-los livremente, sem necessidade de anuência prévia da CONTRATADA.

O detalhamento operacional dos procedimentos necessários à execução dos serviços será formalizado entre a SGGD e a CONTRATADA por meio de playbook(s), a serem elaborados, revisados e acordados após a assinatura do contrato.

A CONTRATADA será responsável por todos os custos de deslocamento, estada e alimentação de seus profissionais envolvidos na prestação dos serviços, assumindo integralmente tais despesas, sem qualquer repasse à SGGD.

Compete à CONTRATADA disponibilizar equipe técnica devidamente capacitada e em número suficiente para atender plenamente às demandas dos serviços contratados, cumprindo os prazos e parâmetros estabelecidos. Deve-se observar rigorosamente o disposto no item 13 - Níveis Mínimos de Serviços exigidos (NMSE) durante toda a vigência do contrato.

Para os serviços de monitoramento contratados, é imprescindível que a CONTRATADA disponibilize equipe especializada, alocando profissionais com os perfis, qualificações e certificações mínimas exigidas pela SGGD, sendo de responsabilidade da CONTRATADA manter estas condições obrigatórias ao longo de toda a vigência do contrato.

12. CRONOGRAMA DE EXECUÇÃO CONTRATUAL

O Cronograma de Execução Contratual estabelece os prazos máximos para cada etapa da implementação dos serviços e soluções contratadas, detalhando as fases macro previstas para garantir a organização, o cumprimento das obrigações contratuais e a efetividade das atividades.

PRAZO	ETAPA
D + 0	Assinatura do contrato
D0 + 5 dias úteis	Reunião de Kickoff do projeto
D0 + 5 dias úteis	Visita de reconhecimento ao espaço físico SGGD
D0 + 10 dias úteis	Entrega do Plano de atuação, contendo minimamente: Profissionais que atuarão com devidas certificações, Modelos de entrega, Soluções utilizadas e cronograma de atuação.
D0 + 15 dias úteis	Entrega do Plano de Sala de Monitoramento SGGD (Planta Baixa)
D0 + 15 dias úteis	Entrega da Solução SIEM
D0 + 25 dias úteis	Instalação e configuração da Solução SIEM
D0 + 30 dias úteis	Início da Operação – Sala de Monitoramento da Contratada

D0 + 60 dias úteis	Entrega do primeiro ciclo de relatórios
D0 + 60 dias úteis	Entrega da Sala de Monitoramento SGGD
D0 + 70 dias úteis	Operacionalização completa das Salas colaborativas de Monitoramento

13. NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS (NMSE)

A CONTRATADA deverá atender aos prazos e prazos máximos estabelecidos no contrato, respeitando os seguintes níveis mínimos:

· Disponibilidade mínima de 99,8% mensal para os serviços contratados, monitorada e calculada com base no tempo total de atividades durante o período. Ocorrências que resultarem em indisponibilidade devem ser documentadas detalhadamente em relatórios;

· Atendimento técnico em horário comercial ou em regime 24x7, conforme especificado pela SGGD, com compromisso de comunicação imediata em caso de falhas ou incidentes críticos (ex. indisponibilidade ou comprometimento das ferramentas).

Gerenciamento de Incidentes e Resposta a Problemas de Segurança: Todas as atividades deverão ser conduzidas com base em frameworks de boas práticas, como NIST CSF, devendo atender às seguintes normas mínimas:

· Classificação de incidentes por criticidade (exemplo: baixa, média, alta e crítica). Incidentes classificados como "críticos" devem ser registrados imediatamente e respondidos no prazo máximo de 30 minutos a partir da detecção ou notificação;

· Problemas classificados como "alta criticidade" deverão ser resolvidos no prazo máximo de 4 horas e notificados formalmente à SGGD;

· A CONTRATADA deverá implementar um sistema de registro de incidentes (ticketing), que permita consulta por parte da SGGD em tempo real e acompanhe a resolução.

A CONTRATADA deverá realizar o monitoramento, reporte e solicitações, para:

· Garantir monitoramento contínuo (24x7) de infraestrutura, ferramentas e serviços relacionados ao contrato;

· Gerar relatórios periódicos de desempenho e incidentes, incluindo:

· Registro detalhado de ocorrências e tempo de resolução;

· Indicadores de desempenho do serviço (KPIs);

· Medidas preventivas e corretivas implantadas no período.

· Atender às solicitações adicionais relacionadas a ajustes e atualizações de ferramentas no prazo máximo de 48 horas úteis, salvo casos que demandem esforço técnico maior, devidamente formalizados e aprovados pela SGGD.

Para garantir a adequação técnica e segurança:

· As ferramentas e soluções ofertadas pela CONTRATADA deverão estar devidamente atualizadas e em conformidade com frameworks de segurança cibernética, como ISO/IEC 27001/27002, NIST CSF e OWASP, reduzindo exposição a vulnerabilidades;

· Implementar medidas proativas, como vulnerabilidade contínua e análise de riscos, para mitigar potenciais ameaças;

· Realizar treinamentos periódicos com as equipes alocadas para garantir a atualização em relação a novas práticas e técnicas de segurança digital.

Sempre que os requisitos especificados deixarem de ser cumpridos, a CONTRATADA estará sujeita à aplicação de descontos no valor mensal da fatura, conforme escalonamento descrito no contrato, proporcional ao impacto gerado para o SGGD.

Parâmetro	**Requisito Mínimo**	**Observação**
Disponibilidade	99,8% mensal	Calculada com base no tempo total de atividades no período. Relatórios detalhados devem ser fornecidos.
Atendimento Técnico	Horário Comercial ou 24x7	Conforme especificado pela SGGD, com comunicação imediata em caso de falhas críticas.
Comunicação de Falhas	Imediata	A CONTRATADA deve informar a SGGD assim que uma falha ou incidente crítico for identificado.

Atividade	**Frequência**	**Conteúdo Mínimo**
Monitoramento Contínuo	24x7	Detecção e resposta a eventos de segurança.
Relatórios de Desempenho	Quinzenal e Mensal	Indicadores de desempenho (KPIs), tempo de resolução, e medidas preventivas/corretivas.
Relatórios de Incidentes	Após cada incidente	Registro detalhado da ocorrência, impacto, ações corretivas e status de resolução.
Atualização de Ferramentas	Sob demanda	Relatório técnico das atualizações realizadas, incluindo versão e compatibilidade.

14. PENALIDADES E GLOSAS POR DESCUMPRIMENTO DE NMSE

A prestação dos serviços será monitorada com base nos indicadores e níveis de serviço acordados. O descumprimento de metas acarretará glosas automáticas e/ou sanções administrativas, conforme segue:

14.1 Indicadores críticos com glosa automática

Ocorrência	Valor da glosa, com base no valor mensal	Limite com base no valor mensal
Incidente **não detectado** que **resultou em exploração**	5% por incidente	20%
Atraso na detecção que **resultou em exploração** ou **indisponibilidade** dos equipamentos do CONTRATANTE	1% por hora	20%
Disponibilidade da Plataforma SOC/SIEM **abaixo** de **99,8%**	5%	
Atraso na emissão dos relatórios	0,5% por dia	5%
Resposta a alertas **críticos** em mais de **30 minutos**	1% por incidente	20%
Resposta a alertas de **alta** criticidade em mais de **45 minutos**	0,5% por incidente	15%
Resposta a alertas de **média** criticidade em mais de **1 hora**	0,1% por incidente	10%
Resposta a alertas de **baixa** criticidade em mais de **4 horas**	0,1% por incidente	5%

14.2 Limite Máximo de Glosa

O total de glosas mensais aplicadas não poderá ultrapassar 30% do valor da fatura mensal. A reincidência por 3 (três) meses consecutivos ou 5 (cinco) meses intercalados em 12 meses será considerada inadimplemento contratual passível de rescisão.

14.3 Procedimento de Apuração

A SGGD notificará a contratada, com apresentação dos dados de monitoramento e evidências. A contratada poderá apresentar manifestação em até 5 (cinco) dias úteis. Após análise, será emitido parecer final e aplicada a glosa no pagamento subsequente.

14.4 Penalidades Cumulativas

As glosas não eximem a contratada da aplicação de sanções previstas na Lei e na minuta contratual, como advertência, suspensão e declaração de inidoneidade, quando aplicável.

15. REQUISITOS DOS SERVIÇOS DE SUPORTE TÉCNICO

O suporte às ferramentas sob gestão da SGGD será de responsabilidade exclusiva da própria SGGD, incluindo ajustes, acionamentos e demais ações necessárias à manutenção dos serviços contratados. Compete à SGGD, sempre que possível, notificar previamente quaisquer indisponibilidades que possam comprometer o funcionamento das ferramentas sob sua responsabilidade.

À CONTRATADA caberá a gestão integral da infraestrutura necessária à execução de suas atividades, incluindo manutenção preventiva e corretiva de eventuais falhas que impactem seus serviços. Deverá, ainda, disponibilizar canais de atendimento eletrônico e/ou telefônico para suporte às atividades contratadas.

Compete à CONTRATADA a geração, distribuição e arquivamento de relatórios, sob demanda ou de forma automática, contendo no mínimo: (i) detalhamento de eventos ou incidentes; (ii) medidas corretivas adotadas e recomendações de prevenção; (iii) indicadores de desempenho (KPIs) definidos contratualmente; e (iv) registros de ocorrências excepcionais.

A CONTRATADA deverá realizar reuniões periódicas de ponto de controle, com frequência previamente acordada entre as partes, para apresentação de relatórios de desempenho, discussão de pendências, revisão de metas e indicadores, e proposição de melhorias nos processos, quando necessário.

Demais ações podem ser acordadas entre a SGGD e a CONTRATADA no decorrer da execução contratual.

16. REQUISITOS DOS SERVIÇOS DE GARANTIAS

A CONTRATADA se compromete a prestar os serviços conforme estabelecido no contrato, observando integralmente os prazos, regras, obrigações e níveis de serviço (SLAs), assegurando a qualidade. O descumprimento injustificado dos prazos acarretará a aplicação de desconto proporcional no valor da fatura da CONTRATADA, conforme critérios previamente definidos no contrato, considerando a gravidade e os impactos do atraso na execução dos serviços.

Os prazos estabelecidos poderão ser flexibilizados somente em circunstâncias excepcionais ocasionadas por fatores alheios à responsabilidade da CONTRATADA, como indisponibilidades de serviços e ferramentas sob responsabilidade da SGGD. Nessas situações, deverão ser seguidas as condições: A SGGD deverá notificar formalmente a CONTRATADA sobre as indisponibilidades que impactem a execução das atividades; A CONTRATADA deverá formalizar o pedido de flexibilização dos prazos, indicando os impactos específicos e o novo cronograma sugerido; A aceitação ou ajuste dos novos prazos será acordada formalmente entre ambas as partes.

17. QUALIFICAÇÕES DOS PERFIS PROFISSIONAIS

Responsável (Supervisor/Líder) pelo Monitoramento

O profissional que atuará como Supervisor/Líder de Monitoramento deve possuir competências gerenciais e sólidos conhecimentos técnicos, especialmente nas áreas de segurança da informação, redes, blue team e red team. Ele será responsável por garantir a gestão do contrato como um todo, promovendo a execução eficaz das atividades contratadas conforme os cronogramas e critérios de qualidade definidos. O

líder também deverá intervir em atividades específicas, diagnosticando problemas de execução e conduzindo ações corretivas que assegurem o pleno desempenho e alinhamento entre a CONTRATADA e o SGGD. Outras responsabilidades incluem a coordenação e acompanhamento das equipes de SOC N1, com ênfase na aplicação de boas práticas de segurança da informação (ISO/IEC 27001, NIST CSF ou outras), bem como a comunicação e elaboração de relatórios para informar sobre o desempenho, a identificação de riscos e os resultados da equipe de monitoramento.

A qualificação mínima para este cargo exige Ensino Superior completo em Informática, Administração ou equivalente com especialização em Tecnologia da Informação ou área correlata, cuja especialização tenha carga horária mínima de 360 horas. É requerida uma experiência mínima de 36 meses de atuação em atividades similares ao perfil descrito. As certificações recomendadas (desejáveis) na área de segurança da informação e gestão de infraestruturas incluem CompTIA Security+, CISM, ITIL, CEH ou equivalentes. Em termos de habilidades interpessoais, o profissional deve demonstrar liderança, capacidade de resolução de conflitos e comunicação eficaz, qualidades essenciais para gerenciar equipes e alinhar processos ao escopo contratual.

Operador de Monitoramento / Analista de Cibersegurança Pleno

O Operador de Monitoramento ou Analista de Cibersegurança Pleno será responsável por executar as atividades de monitoramento de SOC, garantindo a detecção e resposta a eventos de segurança de TI gerados pelos sistemas da SGGD. Este profissional deverá identificar, registrar e tratar eventos ou incidentes de segurança da informação, conforme procedimentos descritos nos playbooks e roteiros providos pela SGGD. Cabe a ele propor ações preventivas e corretivas para garantir a segurança do ambiente monitorado e a mitigação de riscos, além de assegurar a documentação clara e precisa de todos os eventos tratados e gerar relatórios sobre atividades de monitoramento e incidentes gerenciados.

Para este perfil, a qualificação mínima requer Ensino Superior completo ou tecnólogo em áreas como Informática, Análise e Desenvolvimento de Sistemas, Gestão de TI ou áreas correlatas. É exigida uma experiência mínima de 24 meses de atuação em atividades semelhantes ao perfil descrito no contrato. As certificações recomendadas (exigidas) incluem certificações técnicas na área de segurança, como CompTIA Security+, ISO/IEC 27001 Foundation, Microsoft Security Operations Analyst ou outras relacionadas ao ambiente de SOC e monitoramento. Certificações que demonstrem domínio de ferramentas de SOC (ex.: SIEM) são consideradas diferenciais relevantes. As competências técnicas requeridas abrangem boa capacidade de análise e habilidade em ferramentas de monitoramento de segurança, como SIEM (Security Information and Event Management), firewalls e sistemas antivírus, além de conhecimento atualizado em metodologias de gerenciamento e análise de incidentes de segurança e familiaridade com frameworks de cibersegurança, como NIST CSF e MITRE ATT&CK.

Prestadores de Serviços

A SGGD poderá solicitar a substituição de profissionais a qualquer momento caso seja constatado que a equipe, como um todo, não possui as competências técnicas exigidas nos perfis, ou se algum integrante da equipe apresentar conduta inadequada, conforme o código de ética, procedimentos de segurança estabelecidos ou políticas de sigilo de informações da SGGD. Nesses casos, a CONTRATADA deverá providenciar, no prazo máximo de 7 (sete) dias úteis, um profissional substituto que atenda aos requisitos contratuais, com as mesmas ou melhores qualificações exigidas para o cargo, sem qualquer custo adicional à SGGD.

A CONTRATADA deverá comprovar que, no mínimo, 50% dos seus colaboradores operacionais alocados para o monitoramento do SOC N1 possuem, ao menos, uma certificação técnica relacionada à segurança de TI e dois cursos de capacitação técnica nas soluções listadas abaixo. Caso a CONTRATADA opte por sugerir soluções não especificadas na lista, estas deverão ser previamente aprovadas pela SGGD.

A CONTRATADA deverá demonstrar os conhecimentos práticos de sua equipe em pelo menos duas das seguintes categorias:

· IPS (Intrusion Prevention System): Conhecimento em soluções como Sourcefire, McAfee, Trend Micro, ISS ou outras de grande relevância no mercado aceitas pela SGGD.

· EDR: Expertise em soluções como Trend Micro, Crowdstrike, SentinelOne ou outras de grande relevância aceitas pela SGGD.

· Firewall: Domínio de tecnologias como Check Point, Fortinet, Palo Alto ou outras de grande relevância no mercado aceitas pela SGGD.

· Proteção contra DDoS: Habilidade com soluções como Arbor, Radware, F5 ou outras de grande relevância no mercado aceitas pela SGGD.

· Balanceamento de Carga: Familiaridade com tecnologias como F5, Citrix, A10 ou outros equivalentes aceitos pela SGGD.

· Filtragem de E-mails: Conhecimento em soluções como Symantec, McAfee, IronPort, Trend Micro ou outras de grande relevância aceitas pela SGGD.

· Filtro de Conteúdo Web: Experiência com soluções como Symantec, McAfee, IronPort ou outras equivalentes aceitas pela SGGD.

18. REQUISITOS DOS SERVIÇO DE INSTALAÇÃO

Configuração e integração de hardware e software necessários ao funcionamento das ferramentas e soluções necessárias para o Centro de Operações de Segurança - Monitoramento de Incidentes Cibernético;

· Integrações as conexões físicas e lógicas à rede da SGGD, devendo estas estar alinhadas aos requisitos técnicos e de segurança fornecidos pela SGGD;

· Adequação das ferramentas e soluções utilizadas às normas e boas práticas de segurança da informação, tais como as descritas em frameworks como ISO/IEC 27001 e NIST CSF.

A CONTRATADA deverá apresentar, no cronograma de execução contratual após a assinatura do contrato, com um plano detalhado contendo:

· Cronograma de instalação, prevendo etapas, prazos e recursos alocados;

· Lista de ferramentas e componentes que serão instalados;

· Identificação de eventuais dependências relacionadas à SGGD e prazos para sua resolução.

· A instalação completa deverá ser concluída no prazo cronograma de execução contratual a partir da autorização formal por parte da SGGD. Eventuais atrasos deverão ser previamente justificados e formalmente aprovados pela SGGD.

Com a conclusão da instalação, a CONTRATADA deverá realizar testes para validar o funcionamento dos componentes instalados. Esses testes deverão:

· Ser realizados em conjunto com a equipe designada pela SGGD e obedecer aos critérios previamente acordados no contrato;

· Garantir a plena funcionalidade das ferramentas e a conformidade com os requisitos de segurança e desempenho especificados pela SGGD;

· Ser documentados em relatórios técnicos completos e apresentados em até cronograma de execução contratual após a finalização da instalação.

A SGGD deverá formalizar a aceitação da instalação mediante aprovação do relatório técnico ou notificar a CONTRATADA, caso sejam necessárias correções ou adequações.

A CONTRATADA deverá entregar à SGGD toda a documentação técnica da instalação, contemplando:

· Configurações realizadas, incluindo parâmetros utilizados nas ferramentas e equipamentos;

· Manuais de utilização e procedimentos de manutenção preventiva e corretiva;

· Relatórios de testes realizados e validações;

· Informações detalhadas para auditoria, garantindo rastreabilidade de todas as ações realizadas durante o processo de instalação.

19. REQUISITOS E ASPECTOS DE SEGURANÇA

19.1 Confidencialidade e sigilo das informações

A CONTRATADA compromete-se, por si e por seus representantes, a manter absoluto sigilo e confidencialidade sobre todas as informações e documentos acessados em razão da execução dos serviços, sendo vedada sua divulgação, total ou parcial, por qualquer meio, salvo mediante autorização expressa da SGGD. O acesso a tais informações será permitido apenas a colaboradores diretamente envolvidos nas atividades, desde que respeitadas as normas internas de segurança. Em caso de quebra de sigilo ou uso indevido das informações, a CONTRATADA responderá integralmente, inclusive por atos de seus prepostos, conforme as penalidades previstas no contrato e na legislação aplicável.

19.2 Controle de acesso físico e lógico

A SGGD realizará a análise prévia de todas as solicitações da CONTRATADA relacionadas à liberação de acessos indispensáveis à execução dos serviços, abrangendo ambientes físicos, equipamentos, softwares e sistemas. Para tanto, a CONTRATADA deverá apresentar, antecipadamente, toda a documentação e informações necessárias, em conformidade com as políticas de segurança estabelecidas pela SGGD.

O acesso a dependências físicas e lógicas será restrito, monitorado e condicionado ao estrito cumprimento das normas internas de controle e segurança. Qualquer solicitação de novo acesso ou alteração de acessos existentes deverá ser formalmente justificada pela CONTRATADA, com exposição clara da necessidade.

19.3 Obediência às políticas de segurança

A CONTRATADA deverá assegurar que todos os seus empregados e representantes:

· Estejam cientes das políticas de segurança em vigor no SGGD;

· Respeitem e cumpram essas políticas de forma integral durante todas as atividades realizadas.

O SGGD atualizará a CONTRATADA sobre quaisquer alterações nas políticas de segurança, sendo de responsabilidade da CONTRATADA adaptar-se prontamente às novas diretrizes e disseminá-las internamente à sua equipe. Qualquer violação às políticas de segurança será informada à SGGD de forma imediata e corrigida sem impacto financeiro para o SGGD.

19.4 Medidas de segurança da informação e dados

As solicitações da CONTRATADA relativas à liberação de acessos necessários à execução dos serviços, incluindo acesso a dependências físicas, equipamentos, softwares e sistemas, serão previamente analisadas pela SGGD. Caberá à CONTRATADA fornecer, de forma antecipada, toda a documentação e as informações exigidas para viabilizar a liberação, em conformidade com os normativos definidas pela SGGD.

O acesso a ambientes físicos e lógicos será restrito, monitorado e condicionado ao cumprimento integral das normas internas de controle e segurança estabelecidas. Solicitações de novos acessos ou alterações nos acessos previamente autorizados deverão ser formalmente justificadas pela CONTRATADA, mediante apresentação de motivação adequada.

19.5 Atendimento “On-Site”

A disponibilização de profissionais para atendimento presencial ("on-site") será condicionada ao cumprimento estrito das políticas da SGGD. OS profissionais deverão atender a todos os critérios de acesso físico estabelecidos pelo SGGD, incluindo:

· Cadastro prévio e autorização formal para trânsito em áreas restritas;

· Uso de crachás e equipamentos de identificação, quando exigidos;

· Obediência às normas comportamentais e de conduta determinadas.

O controle de entrada, permanência e saída desses profissionais será realizado com base nas diretrizes internas de segurança do SGGD.

20. MODELO DE GESTÃO DO CONTRATO

A execução e fiscalização do contrato serão realizadas por meio de um gestor ou equipe de fiscalização composta por servidores da CONTRATANTE, formalmente designados pela SGGD. Compete a esses representantes verificarem a conformidade da prestação dos serviços, garantindo o fiel cumprimento do contrato, promovendo o registro de ocorrências e adotando as medidas necessárias, conforme a legislação aplicável e as normativas do BID.

As atividades de gestão e fiscalização devem ser exercidas de forma preventiva, rotineira e sistemática, por servidor ou equipe de fiscalização, desde que seja assegurada a separação entre as funções e que o volume de trabalho não comprometa a execução adequada das atribuições relativas à gestão contratual. Durante a execução do objeto, o fiscal técnico deverá monitorar continuamente o nível de qualidade dos serviços prestados, intervindo sempre que necessário para exigir da Contratada a correção de falhas, omissões ou irregularidades identificadas.

A atuação da fiscalização não exime a CONTRADADA de suas responsabilidades, inclusive perante terceiros, por quaisquer irregularidades decorrentes de imperfeições técnicas, vícios redibitórios ou uso de materiais inadequados ou de qualidade inferior, tampouco implica corresponsabilidade da Contratante ou de seus representantes.

20.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

20.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

20.3. As comunicações entre o Contratante e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

20.4. O Contratante poderá convocar representante do Contratado para adoção de providências que devam ser cumpridas de imediato.

20.5. Após a celebração da contratação, o Contratante poderá convocar o representante do Contratado para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do Contratado, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Preposto

20.6. O Contratado designará formalmente o seu preposto, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

20.7. O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto do Contratado, hipótese em que o Contratado designará outro para o exercício da atividade.

Fiscalização

20.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelo(s) respectivo(s) substituto(s) (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

20.9. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração (Decreto estadual nº 68.220, de 15 de dezembro de 2023, art. 17).

20.10. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133, de 2021, art. 117, §1º e Decreto estadual nº 68.220, de 2023, art. 17, II).

20.11. O fiscal técnico realizará, em conformidade com cronograma físico-financeiro, as medições dos serviços executados e aprovará a planilha de medição emitida pelo Contratado (Decreto estadual nº 68.220, de 2023, art. 17, inciso III).

20.12. O fiscal técnico adotará medidas preventivas de controle de contratos, manifestando-se quanto à necessidade de suspensão da execução do objeto (Decreto estadual nº 68.220, de 2023, art. 17, inciso IV).

20.13. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso (Lei nº 14.133, de 2021, art. 117, § 2º).

20.14. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato (Decreto estadual nº 68.220, de 2023, art. 17, inciso II).

Fiscalização Administrativa

20.15. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Decreto estadual nº 68.220, de 2023, art. 18, II e III).

20.16. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência (Decreto estadual nº 68.220, de 2023, art. 18, IV).

20.17. Sempre que solicitado pelo Contratante, o Contratado deverá comprovar o cumprimento da reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, com a indicação dos empregados que preencherem as referidas vagas, nos termos do parágrafo único do art. 116 da Lei nº 14.133, de 2021.

Gestor do Contrato

20.18. O gestor do contrato exercerá a atividade de coordenação dos atos de fiscalização técnica, administrativa e setorial e dos atos preparatórios à instrução processual visando, entre outros, à prorrogação, à alteração, ao reequilíbrio, ao pagamento, à eventual aplicação de sanções e extinção do contrato (Decreto estadual nº 68.220, de 2023, inciso III do art. 2º).

20.19. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais (Decreto estadual nº 68.220, de 2023, art. 16, inciso IX).

20.20. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações (Decreto estadual nº 68.220, de 2023, art. 16, inciso VI).

20.21. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso (Decreto estadual nº 68.220, de 2023, art. 16, inciso VIII).

20.22. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração (Decreto estadual nº 68.220, de 2023, art. 16, inciso VII e parágrafo único).

20.23. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

21. CONDIÇÕES DE PAGAMENTO

21.1 Acionamento, aferição e condições de pagamento

Serviços de Centro de Operações de Segurança - Monitoramento de Incidentes Cibernético

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da prestação do serviço será realizada por meio da disponibilização de um relatório mensal das atividades, conforme os itens específicos de relatórios e demais atividades estabelecidas neste Termo de Referência.

· Métrica: Serviço / Mês.

· Forma de pagamento: Mensal. Solução SIEM / SOAR

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório detalhado, contendo evidências da disponibilização e instalação da ferramenta.

· Métrica: EPS.

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Solução EDR

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório detalhado, contendo evidências da disponibilização e instalação da ferramenta.

· Métrica: Unidade (número de endpoints protegidos)

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Solução EPM

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório detalhado, contendo evidências da disponibilização e instalação da ferramenta.

· Métrica: Unidades instaladas

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Solução Anti-Ransomware

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório detalhado, contendo evidências da disponibilização e instalação da ferramenta.

· Métrica: Unidades instaladas

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Solução de Threat intelligence

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório detalhado, contendo evidências da disponibilização e instalação da ferramenta.

· Métrica: EPS e Cobertura de fontes monitoradas (OSINT/Deep/Dark Web) e Takedown de sites maliciosos/fraude

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Solução CSPM (Cloud Security Posture Management)

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório detalhado, contendo evidências da disponibilização da ferramenta, das integrações com os ambientes em nuvem e da execução inicial de varreduras de conformidade.

· Métrica: Ambientes/Nuvens monitoradas e número de verificações de conformidade executadas

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Solução WAF (Web Application Firewall)

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório detalhado, contendo evidências da instalação da solução, configuração das políticas de proteção e início do monitoramento ativo das aplicações web protegidas.

· Métrica: Número de aplicações web protegidas

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Solução Pentest (Teste de Intrusão)

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da entrega da solução será realizada por meio de um relatório técnico e executivo detalhado, contendo evidências dos testes realizados, metodologias aplicadas, vulnerabilidades identificadas e recomendações de mitigação.

· Métrica: Quantidade de ativos avaliados e escopos testados (aplicações, redes, infraestrutura)

· Forma de pagamento: Pagamento único, a ser efetuado após a homologação da entrega. Serviço de Resposta a Incidentes (N1, N2 e Serviço especializado N2 e N3)

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição da prestação do serviço será realizada por meio da disponibilização de um relatório mensal das atividades executadas, contendo as respectivas horas especializadas consumidas.

· Métrica: Hora Especializada.

. Forma de pagamento: Mensal, condicionado à homologação das horas consumidas, sendo um serviço sob demanda. Salas Físicas

· O acionamento será efetuado após a assinatura do contrato e seguirá o cronograma de execução contratual.

· A aferição será realizada de forma única, no início da operação do Centro de Operações de Segurança - Monitoramento de Incidentes Cibernético e resultará na cobrança mensal do valor correspondente às Salas Físicas de Monitoramento.

· Métrica: Unidade.

· Forma de pagamento: Pagamento único, a ser efetuado após a instalação.

As notas fiscais somente poderão ser emitidas após o ateste realizado pelo fiscal do contrato, em até 10 (dez) dias úteis após o recebimento dos produtos e relatórios, sendo exigido novo envio em caso de incorreções. Ao término do contrato, a CONTRATADA deverá, no prazo de

até 30 (trinta) dias corridos após solicitação formal do CONTRATANTE, desinstalar e remover, por sua conta e risco, todos os equipamentos e bens de sua propriedade, incluindo a desmontagem completa da Sala de Monitoramento de Segurança da Informação (Sala I – SGGD), sem quaisquer ônus à SGGD. A permanência desses bens após o encerramento contratual não gerará custos adicionais por parte da SGGD.

21.2 Prazo de pagamento

O pagamento será realizado em até 30 (trinta) dias contados após a apresentação da nota fiscal ou documento equivalente, desde que concluída a liquidação da despesa, nos termos do art. 2º, II, do Decreto estadual nº 67.608/2023. Em caso de atraso, os valores serão atualizados monetariamente conforme a legislação vigente, com aplicação de juros moratórios de 0,5% ao mês, calculados pro rata temporis, conforme o art. 2º, III, do Decreto nº 67.608/2023, combinado com o art. 1º do Decreto nº 32.117/1990.

21.3 Forma de pagamento

O pagamento será efetuado por meio de ordem bancária, mediante depósito em conta corrente em nome do CONTRADO no Banco do Brasil S/A. Constitui condição para a realização dos pagamentos a inexistência de registros em nome do CONTRATADO no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais– CADIN ESTADUAL”, salvo se comprovada a suspensão dos registros, nos termos do artigo 8º da Lei estadual nº12.799, de 2008.A data de pagamento corresponderá à emissão da ordem bancária. Sendo que o CONTRATANTE poderá, por ocasião do pagamento efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

22. MATRIZ DE RISCOS

Risco Identificado	Categoria	Probabilidade	Impacto	Nível de Criticidade	Consequência	Plano de Ação (Medidas de Mitigação)	Responsável	Status
Indisponibilidade de sistemas operacionais	Operacional	Alta	Alto	Crítico	Paralisação total ou parcial dos serviços críticos de segurança e perda de visibilidade sobre eventos de segurança.	Implementar redundância de sistemas, monitoramento proativo (24x7), testes de capacidade e failover.	TI / Infraestrutura	Planejado
Ataque de Ransomware com impacto em dados críticos	Cibernético	Média	Crítico	Crítico	Criptografia e sequestro de dados, resultando em interrupção operacional e riscos à reputação	Aplicar atualizações periódicas em sistemas, backup diário externo e campanhas de conscientização.	Segurança da Informação	Em andament
Vazamento de dados sensíveis de clientes ou contratos	Cibernético	Média	Crítico	Crítico	Exposição de informações confidenciais, danos à imagem e sanções legais	Implementar criptografia ponta-a-ponta em dados confidenciais; controle de acesso e monitoramento.	TI / Segurança da Informação	Em análise
Falha humana no envio de informações sigilosas ao destinatário errado	Humano	Alta	Moderado	Alto	Exposição acidental de dados sensíveis com impacto jurídico e reputacional	Treinamento contínuo de colaboradores e aplicação de política de dupla verificação para envio de dados.	RH / Operações	Planejado
Descumprimento das políticas internas de segurança (não seguir normas da SGGD)	Humano	Média	Alto	Alto	Risco de falhas em processos críticos e não conformidade com auditorias e normas internas	Aplicar medidas disciplinares e treinar colaboradores na adequação às normas de segurança da SGGD.	RH / Compliance	Concluído
Ataque DDoS contra servidores críticos de operação	Cibernético	Baixa	Alto	Moderado	Interrupção parcial ou total dos serviços prestados pelo SOC, afetando a detecção de ameaças	Implementar soluções de proteção contra DDoS (Arbor, Radware) e realizar testes simulados de ataque.	TI / Infraestrutura	Planejado

Indisponibilidade da equipe técnica ou de suporte	Operacional	Média	Moderado	Moderado	Lentidão ou falhas na resposta a incidentes e manutenção de sistemas	Criar plano de escalonamento de equipes, com suporte de pessoal em redundância ou outsourcing emergencial.	RH e Gestão de Pessoas	Em andamento
Vulnerabilidade no acesso remoto de colaboradores	Cibernético	Alta	Moderado	Alto	Possibilidade de acesso não autorizado aos sistemas e exposição de dados sensíveis	Aplicar autenticação multifator (MFA), revisão constante de acessos privilegiados e monitoramento.	Segurança da Informação	Em análise
Atrasos na entrega de relatórios periódicos à SGGD	Operacional	Média	Baixo	Moderado	Comprometimento da conformidade regulatória e atrasos na tomada de decisão estratégica	Implementar controle automatizado de prazos para a geração/validação de relatórios no sistema interno.	TI / Operações	Planejado

Definição dos campos

· Risco Identificado: Descrição do risco que pode prejudicar os serviços, sistemas ou informações.

· Categoria: Classificação em Operacional, cibernético, humano ou qualquer outro tipo aplicável.

· Probabilidade: Probabilidade de ocorrência (Baixa, Média, Alta), ajustada conforme os parâmetros do framework.

· Impacto: Consequências esperadas do risco (Baixo, Moderado, Alto, Crítico).

· Nível de Criticidade: O nível de prioridade do risco, definido pelo cruzamento entre probabilidade e impacto.

· Consequência: Possíveis consequências associadas aos riscos.

· Detalhamento dos possíveis efeitos negativos caso o risco se materialize.

· Plano de Ação (Medidas de Mitigação): Conjunto de medidas proativas ou reativas para evitar ou tratar o risco.

· Responsável: Área ou equipe designada para evitar ou gerenciar o risco.

· Status: Progresso do tratamento do risco (Planejado, em andamento, em análise, Concluído). Análise da criticidade

A criticidade de um risco é obtida cruzando a probabilidade com o impacto:

· Alta probabilidade + Alto impacto → Risco Crítico.

· Média probabilidade + Alto impacto → Risco Alto.

· Baixa probabilidade + Alto impacto → Risco Moderado.

· Baixa probabilidade + Baixo impacto → Risco Aceitável.

23. VIGÊNCIA CONTRATUAL

A contratação terá vigência de 12 (doze) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos sucessivos durante a vigência do contrato de empréstimo (5579/OC-BR), observado o limite e as condições previstas na Lei nº 14.133/2021.

A execução dos serviços deverá ocorrer preferencialmente dentro da vigência contratual, respeitados os prazos estabelecidos no cronograma apresentado.

A vigência poderá ser encerrada de forma antecipada nas hipóteses previstas em lei, especialmente em caso de descumprimentos das obrigações impostas, interesse público devidamente motivado, ou por razões de conveniência administrativa.

ANEXO II

ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS - ESP N.º E0250354

Este documento, a partir de sua assinatura, fará parte integrante do Contrato de Prestação de Serviços **PD025290,** firmado com a **SECRETARIA DE GESTAO E GOVERNO DIGITAL - SGGD**

OBJETO

Prodesp Shield e SOC

ESCOPO DA PRESTAÇÃO DE SERVIÇOS

O Prodesp Shield é um serviço de segurança cibernética que protege as informações e sistemas ativos digitais contra ameaças e ataques cibernéticos. Ele funciona como uma série de barreiras de proteção, cada uma com uma função específica, como proteger a rede de computadores, os aplicativos usados pela empresa, os dispositivos dos funcionários e os dados sensíveis.

Os serviços de Prodesp Shield consistem em um conjunto integrado de tecnologias avançadas em segurança da informação, organizadas em camadas, proporcionando uma proteção abrangente e completa contra ameaças cibernéticas.

A solução é aplicada com base no modelo de camadas de Segurança Digital, considerando que cada uma das camadas trabalha em conjunto para criar uma defesa em profundidade, onde múltiplas barreiras protegem contra diferentes tipos de ameaça cibernética.

Nesta Especificação de Serviços e Preços - ESP estão contempladas as seguintes camadas:

Camada Endpoint

o Proteção abrangente com foco na segurança de endpoints contra ameaças cibernéticas, incluindo detecção e respostas avançadas

Camada Ativos de Missão Crítica

o Ativos de Missão Crítica atuam na proteção contra ameaças e roubo de credenciais com segurança em camadas e gerenciamento de privilégios

Gestão DOP

o Serviços de Gerenciamento de Operações – Prata

Recursos adicionais (PaaS Middleware)

o Plataforma integrada de operações de segurança (SOC)

o SIEM e SOAR

o EPM (Endpoint Privilegie Management)

o Anti-Ransonware

o CSPM (Cloud Security Posture Management)

o WAF (Web Application Firewall)

o Pentest

o CTI (Cyber Threat Intelligence)

o Gestão da Qualidade

o Serviços

o Sala de SOC

Serviços

As atividades do SOC serão realizadas em colaboração entre a CONTRATADA e a SGGD. As responsabilidades serão detalhadas no plano de atuação pós-contrato.

2.1. **Camada: Endpoint**

2.1.1. Serviço de Detecção e Resposta Estendida para Estações de Trabalho

Solução de proteção para estações de trabalho, notebooks e desktops, integrada à plataforma de detecção e resposta estendida.

Este serviço contempla:

·Proteção avançada baseada em machine learning (aprendizado de máquina - é um método de análise de dados que automatiza a construção de modelos analíticos);

·Identificação de ameaças baseada em análise comportamental;

·Detecção de ataques em memória;

·Anti-malware de próxima geração;

·Firewall de host (firewall em software que realiza o bloqueio de tráfego indesejado no dispositivo do usuário);

·Controle de aplicações;

o Identificação e blindagem de vulnerabilidades;

o Autoproteção do agente;

·Controle de dispositivos externos (USB, pen-drive, HD externo);

·Endpoint detection and response – EDR (Detecção e Resposta de Endpoint);

·Integração nativa com a plataforma de detecção e resposta estendida - XDR

2.1.1.1. **Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos;**

·Administração centralizada da plataforma de detecção e resposta estendida:

·Atualização automática do software de segurança;

·Verificação periódica e em tempo real, visando a detecção de ameaças conhecidas e desconhecidas nas estações de trabalho e servidores;

·Auxílio para solucionar as ocorrências de vírus, malwares e exploits;

·Identificação de ameaças ou suspeita de contaminação do ambiente corporativo;

·Comunicação de incidências de vírus e de ameaças de computador desconhecidas.

2.1.1.2. **Entregáveis**

·Relatórios contemplando evidências mapeamento de exploração de vulnerabilidades, quantidade de ameaças bloqueadas, potenciais vulnerabilidades presentes em endpoints, MTTD, MTTR, e demais indicadores a serem acordados em tempo de projeto;

·Relatório contemplando os principais dispositivos e aplicações com risco;

·Os relatórios serão emitidos com visões alinhadas com os níveis de serviço, sendo elas “Operacional”, “Gerencial” e “Executivo”.

·A geração dos relatórios seguirá as melhores práticas de mercado.

2.1.1.3. **Pré-requisitos**

·Sistema Operacional:

o Windows 10 (32bit e 64bit);

o Windows 11 (32bit e 64bit);

o CentOS 5 e 6 (32bit e 64bit);

o CentOS 7, 8 (64bit);

o Debian 7 ou superior (64bit);

o Ubuntu 16.04 ou superior;

o Amazon Linux 1 ou superior;

o CloudLinux 7 ou superior;

o AlmaLinux 8 ou superior;

·Processador:

o Mínimo 2.0 GHz Intel Pentium ou equivalente (4-core);

·Memória (RAM):

o Mínimo de 3GB exclusivamente para o agente da solução em desktops;

·Espaço de disco:

o Mínimo de 5GB.

2.1.1.4. **Suporte Técnico**

·O serviço de suporte técnico será realizado remotamente em regime 24x7.

2.1.1.5. **Horário de atendimento**

SLA	**Detecção**	**Contenção**	**Resposta**
Bronze [N1]	Até 4 horas	Até 8 horas	Até 12 horas
Prata [N2]	Até 2 horas	Até 4 horas	Até 8 horas
Ouro [N3]	Até 30 minutos	Até 1 hora	Até 4 horas

2.2. **Camada: Ativos de Missão Crítica**

2.2.1. Serviço de Detecção e Resposta Estendida para Servidores

Solução avançada de proteção para servidores fiscos, virtuais e em nuvem, integrada à plataforma de detecção e resposta estendida.

Este serviço contempla:

·Proteção avançada baseada em machine learning (aprendizado de máquina - é um método de análise de dados que automatiza a construção de modelos analíticos);

·Identificação de ameaças baseada em análise comportamental;

·Detecção de ataques em memória;

·Antimalware de próxima geração;

·Bloqueio de ameaças via web reputation;

·Firewall de host (firewall em software que realiza o bloqueio de tráfego indesejado no dispositivo do usuário);

·Controle de aplicações;

·Monitoramento da integridade de arquivos, registros, bibliotecas e DLL do sistema operacional;

·Inspeção profunda dos logs do Sistema Operacional.;

·Identificação e blindagem de vulnerabilidades;

·Autoproteção do agente;

·Controle de dispositivos externos (USB, pen drive, HD externo);

·Integração nativa com a plataforma de detecção e resposta estendida.

2.2.1.1. **Atividades previstas**

·Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos;

·Administração centralizada da plataforma de detecção e resposta estendida:

o Atualização automática do software de segurança;

o Verificação periódica e em tempo real, visando a detecção de ameaças conhecidas e desconhecidas nas estações de trabalho e servidores;

·Auxílio para solucionar as ocorrências de vírus, malwares e exploits;

·Identificação de ameaças ou suspeita de contaminação do ambiente corporativo;

·Comunicação de incidências de vírus e de ameaças de computador desconhecidas.

2.2.1.2. **Entregáveis**

·Relatórios mensais contemplando evidências mapeamento de exploração de vulnerabilidades, quantidade de ameaças bloqueadas, potenciais vulnerabilidades presentes em servidores;

·Relatório mensais contemplando os principais usuários, dispositivos e aplicações com risco;

·Relatório mensal contemplando os principais hosts afetados por ameaças.

2.2.1.3. **Pré-requisitos**

·Sistema Operacional:

o Windows Server 2008 R2 (64bit) ou superior;

o CentOS 6 (64bit) ou superior;

o Debian 10 ou superior (64bit);

o Ubuntu 16.04 (64bit) ou superior;

o Amazon Linux 2 ou superior (64bit);

o Oracle Linux 7 (64bit) ou superior;

o RHEL 6 (64bit) ou superior;

o Suse 12 ou superior;

o CloudLinux 7 ou superior;

o AlmaLinux 8 ou superior.

o Serviços de Gerenciamento de Operações – Ouro (dada a complexidade da operação, foram incluídas nesta demanda duas unidades de gestão Ouro)

·Bloqueio de ameaças via web reputation;

·Relatório contemplando os principais hosts afetados por ameaças.

·O SOC permitirá o acompanhamento ininterrupto de eventos de segurança (24x7) com capacidade de triagem, análise, correlação de alertas, resposta técnica a incidentes.

2.1.1.6. **SLA para Atendimento:**

24 x7 x 365

·Endpoint detection and response – EDR (Detecção e Resposta de Endpoint);

·Processador:

o Mínimo 2.0 GHz Intel Pentium ou equivalente (4-core);

·Memória (RAM):

o Mínimo de 4.5GB.

·Espaço de disco:

o Mínimo de 5GB.

2.2.1.4. **Suporte Técnico**

·O serviço de suporte técnico será realizado remotamente a partir das dependências da Prodesp;

·O SOC permitirá o acompanhamento ininterrupto de eventos de segurança (24x7) com capacidade de triagem, análise, correlação de alertas, resposta técnica a incidentes e acionamento célere das equipes especializadas da Secretaria de Gestão e Governo Digital (SGGD).

2.2.1.5. **Horário de Atendimento:**

SLA	Detecção	Contenção	Resposta
Bronze [N1]	Até 4 horas	Até 8 horas	Até 12 horas
Prata [N2]	Até 2 horas	Até 4 horas	Até 8 horas
Ouro [N3]	Até 30 minutos	Até 1 hora	Até 4 horas

2.3. Gestão DOP

2.3.1. Serviços de Gerenciamento de Operações

·Gestão da documentação fiscal do projeto;

·Elaboração e envio de termos de aceite para fins de faturamento e demonstrativo de atividades realizadas;

·Participação em reunião mensal de governança do projeto, como preposto da PRODESP;

·Elaboração de relatório de Medição para ateste pelo cliente;

·Gestão e Governança de Projetos (Demandas, Escopo, Prazos e Resultados), alinhamento de estratégias, decisões, relatórios de progresso, medições e cronograma do projeto;

·Atuação de arquiteto de infraestrutura junto a equipe para apoio às entregas relativas a integrações, e profissionais de Banco de Dados e Administração de servidores para implementações necessárias;

·Geração de documentação de topologia do projeto;

·Participação nas reuniões de elaboração de Demandas;

2.3.2. **Serviço fora de escopo**

·Gestão e Governança de Equipes: organização dos times de trabalhos e distribuição de tarefas.

·Profissionais dedicados (presenciais) no ambiente do cliente.

2.4. **Recursos Adicionais – Plataforma como Serviço – Paas Middleware**

Este serviço disponibiliza os softwares necessários para continuidade dos serviços implantados e para garantir o correto funcionamento das plataformas, bem como a troca de dados de forma segura entre seus diversos módulos. Estão excluídos deste item os serviços de Plataforma de Banco de Dados (PaaS Oracle e PaaS SQL), bem como os serviços de Plataforma de Aplicações (PaaS JBOSS e PaaS Websphere).

2.4.1. **Recursos Adicionais**

2.4.1.1. Plataforma Integrada de Operações de Segurança (SOC)

Plataforma de visão, identificação e gestão de risco cibernético. Por meio de mapeamento de risco baseado em nove pilares:

·Comprometimento de credenciais;

·Vulnerabilidades;

·Atividade e comportamento;

·Ameaças conhecidas;

·Ameaças avançadas e zero-day;

·Atividade de acesso web e rede local;

·Predição de ataque;

·Configurações incorretas e configurações do sistema;

·Configurações de segurança da plataforma.

2.4.1.1.1. **Atividades Previstas**

·Monitoramento e notificação de alertas e comportamentos suspeitos com base nos pilares citados;

·Verificação periódica e em tempo real, visando a detecção de ameaças conhecidas e desconhecidas;

·Configuração de regras e exceções para melhoria contínua da solução;

·Identificação de usuários com riscos de comprometimento de credenciais;

·Dashboards para acompanhamento dos pilares de risco do ambiente;

·Mapeamento de credenciais vazadas na Darkweb;

·Mapeamento da superfície de ataque passível a ser explorada;

·Identificação de vulnerabilidades, mapeamento de regras de blindagem e recomendações de patches em sistemas e aplicações;

·Identificação de alertas de risco baseados no CSPM (Cloud Security Posture Management), buscando elencar recursos de nuvem expostos e recomendações de melhoria.

2.4.1.1.2. **Entregáveis**

·Relatórios mensais contemplando evidências mapeamento de exploração de vulnerabilidades, quantidade de ameaças bloqueadas e potenciais vulnerabilidades presentes em endpoints, servidores e recursos de nuvem;

·Relatórios mensais com KPIs de risco baseado nos nove pilares, listagem de ações executadas e/ou solicitadas para decréscimo da nota de risco do ambiente;

·Relatórios mensais de saúde do ambiente e plataforma;

·Relatórios mensais de risco com base em contexto de ambiente e panorama executivo.

2.4.1.1.3. **Pré-requisitos**

SLA	**Detecção**	**Contenção**	**Resposta**
Bronze [N1]	**Até 4 horas**	**Até 8 horas**	**Até 12 horas**
Prata [N2]	**Até 2 horas**	**Até 4 horas**	**Até 8 horas**
Ouro [N3]	**Até 30 minutos**	**Até 1 hora**	**Até 4 horas**

2.4.1.2. **SIEM e SOAR**

Os serviços de SIEM (Security Information and Event Management) centralizam e correlacionam logs de múltiplas fontes para detectar ameaças em tempo real, apoiando a análise e resposta a incidentes. Já os serviços de SOAR (Security Orchestration, Automation and response) automatizam tarefas repetitivas, integram ferramentas de segurança e padronizam respostas a incidentes, aumentando a eficiência e reduzindo o tempo de reação. Juntas, oferecem monitoramento inteligente e resposta ágil a ameaças.

Capaz de atender aos mais diversos cenários de ações automatizadas, tais como:

·Reset de senha do usuário diretamente nos serviços de diretórios (AD, Entra ID, OpenLDAP, etc.);

·Sign-out do Usuário;

·Desabilitação do Usuário;

·Isolamento de máquina;

·Bloqueio de IPs, domínios, URLs, Hash & Endereços de E-mail;

·Bloqueio de acesso a aplicações e sites;

·Envio de Script;

·Encerramento de processo;

·Dump de memória;

·Coleta de arquivos e pacotes de rede;

·Escaneamento sob demanda de Malware e IOCs;

·Envio e ingestão de IOCs

2.4.1.2.1. **Atividades Previstas**

·Monitoramento e notificação de alertas, bloqueios de comportamentos suspeitos;

·Auxílio para customização de alertas entre as tecnologias integradas;

·Apoio para criação de playbooks de ações automatizadas;

·Análise de alertas de desvio comportamental direcionados aos usuários, estações de trabalho, servidores e hosts;

2.4.1.2.2. **Entregáveis**

·Relatórios mensais contemplando evidências dos alertas gerados perante as tecnologias integradas, bem como, recomendações de

melhorias nos fluxos de geração de alertas e playbooks;

2.4.1.2.3. **Pré-Requisitos**

·12vCPUs;

·32 GB RAM;

·500 GB Disco;

SLA	Detecção	Contenção	Resposta
Bronze [N1]	**Até 4 horas**	**Até 8 horas**	**Até 12 horas**
Prata [N2]	**Até 2 horas**	**Até 4 horas**	**Até 8 horas**
Ouro [N3]	**Até 30 minutos**	**Até 1 hora**	**Até 4 horas**

O EPM (Endpoint Privilege Management) é uma solução de segurança que aplica o princípio do menor privilégio em servidores.

Ele remove direitos administrativos locais de usuários e aplicações, concedendo privilégios apenas quando necessário, de forma controlada e auditada.

Permite execução segura de softwares autorizados e bloqueia programas não confiáveis.

Fornece rastreabilidade completa das elevações de privilégios, atendendo requisitos de compliance.

O serviço de proteção de credenciais em servidores tem como objetivo proteger os servidores contra-ataques, reduzindo o risco de informações serem roubadas ou criptografadas, como um ataque ransomware, além da prevenção de roubo de credenciais, realizar o bloqueio de instalações de aplicações não autorizadas e elevação de privilégios. Este serviço contempla:

·Proteção contra-ataques de ransomware;

·Eliminação de Privilégios em Servidores;

·Proteção contra roubo de credenciais;

·Bloqueio de instalação de aplicações não autorizadas;

·Restrição de aplicativos baixados da internet;

·Remoção de administradores locais;

·Rotação de senhas locais integrado com o PAM;

·Elevação de privilégio com solicitação de MFA;

·Proteção contra roubo de cookies de navegação.

2.4.1.3.1. **Atividades Previstas**

·Administração centralizada da ferramenta com possibilidade de acesso à console;

·Gestão dos servidores incluindo disparo de atualizações;

·Apoio na configuração de políticas;

·Análise de eventos de comportamento suspeitos.

2.4.1.3.2. **Entregáveis**

·Relatório mensal de eventos de comportamento suspeito;

·Análise dos logs com retorno à CONTRATANTE de como interagir com a solução;

·Relatório de máquinas off-line;

·Relatório de credenciais privilegiadas locais;

·Controle estatístico;

·Relatório gerencial de auditoria de configurações.

2.4.1.3.3. **Pré-requisitos**

·Sistemas Operacionais:

o Windows Server 2016;

o Windows Server 2019;

o Windows Server 2022;

o Red Hat Enterprise Linux 7, 8, e 9;

o SUSE Linux Enterprise 12 e 15;

o Amazon Linux 2;

o CentOS 7;

o Ubuntu 18.04, 20.04, 22.04 e 23.10;

o Oracle Linux 7, 8 e 9.

2.4.1.4. **Anti-Ransonware**

O serviço anti-ransomware utiliza inteligência artificial e machine learning especializados para detectar e bloquear ataques de ransomware, inclusive variantes zero-day. Ela protege contra técnicas avançadas como uso de drivers vulneráveis e ferramentas nativas do sistema, impede desativação de outros controles de segurança e monitora tentativas de exfiltração de dados. Em caso de ataque bem-sucedido, captura chaves de criptografia para permitir restauração automática, reduzindo impacto operacional e eliminando a necessidade de pagamento de resgate, além de oferecer proteção contra adulteração e recursos de isolamento de endpoints.

2.4.1.4.1. **Atividades Previstas**

·Monitoramento contínuo de atividades suspeitas relacionadas a ransomware;

·Detecção comportamental de ataques em tempo real;

·Bloqueio automático de processos maliciosos e reversão de ações de criptografia;

·Análise de artefatos de ransomware e geração de IoCs;

·Apoio à investigação de incidentes com foco em ransomware;

·Atualização contínua de assinaturas e modelos de detecção;

2.4.1.4.2. **Entregáveis**

·Relatórios mensais de detecção de ransomware: detalhamento de eventos bloqueados, artefatos identificados e ações tomadas;

·Dashboards de atividade maliciosa: painéis com indicadores de tentativas de ataque, bloqueios e reversões;

·Documentação de integração: registros técnicos sobre configuração, tuning e integração.

2.4.1.4.3. **Pré-requisitos**

·Inventário de endpoints e ativos críticos;

2.4.1.4.4. **Serviços fora de escopo**

·Remoção manual de ransomware: a ferramenta atua de forma automatizada;

·Administração de infraestrutura de TI: o serviço não contempla configuração de rede, servidores ou políticas de acesso.

2.4.1.4.5. **Suporte Técnico**

·O serviço será operado remotamente, com suporte técnico especializado para integração, tuning e análise de eventos relacionados ao fabricante.

	Detecção	**Contenção**	**Resposta**
Bronze [N1]	**Até 4 horas**	**Até 8 horas**	**Até 12 horas**
Prata [N2]	**Até 2 horas**	**Até 4 horas**	**Até 8 horas**
Ouro [N3]	**Até 30 minutos**	**Até 1 hora**	**Até 4 horas**

2.4.1.5. **CSPM**

Serviços de CSPM (Cloud Security Posture Management) identifica e indica possíveis correções de configurações incorretas em ambientes de nuvem.

2.4.1.6. **Atividades Previstas**

·Serviço de realização de varreduras contínuas para garantir conformidade com frameworks como CIS, NIST e GDPR.

·Fornece visibilidade centralizada sobre riscos e ativos em múltiplos provedores (AWS, Azure, GCP, Huawei e PRODESP).

·Inclui alertas em tempo real e recomendações para remediação automatizada.

·Ajuda a reduzir a superfície de ataque na nuvem, prevenindo violações e acessos não autorizados.

2.4.1.6.1. **Entregáveis**

·Mapeamento e Inventário de Recursos em Nuvem

·Descoberta automática de ativos, serviços e workloads em múltiplos provedores (AWS, Azure, GCP, etc.).

·Classificação por criticidade, tipo de recurso e compliance.

·Avaliação de Postura de Segurança

·Relatórios sobre configuração de segurança da nuvem comparada a benchmarks (CIS, NIST, ISO 27001, PCI DSS, LGPD, etc.).

·Identificação de desvios de boas práticas e falhas de configuração.

·Relatórios de Conformidade e Auditoria

·Relatórios periódicos de compliance (mensais/trimestrais).

·Gap Analysis em relação a regulações aplicáveis.

·Gestão de Vulnerabilidades de Configuração

·Detecção contínua de configurações incorretas (misconfigurations).

·Priorização de riscos baseada em criticidade e impacto potencial.

·Recomendações de remediação detalhadas.

·Monitoramento Contínuo e Alertas.

·Geração de alertas em tempo real sobre violações de políticas de segurança.

·Correlação de eventos críticos de segurança na nuvem.

·Políticas de Segurança Automatizadas

·Aplicação de políticas pré-configuradas e personalizáveis para diferentes ambientes de nuvem.

·Enforcement automático para correção de riscos simples (ex.: bucket S3 público).

·Integração com SIEM/SOAR

·Exportação de eventos e alertas para ferramentas de monitoramento centralizadas.

·Automação de resposta a incidentes (quando aplicável).

·Recomendações de Melhoria Contínua

·Roadmap de maturidade de segurança em nuvem.

·Relatórios executivos (C-Level) e técnicos (Ops/Segurança).

·Indicadores de evolução da postura (KPIs e métricas).

2.4.1.6.2. **Pré-requisitos**

·Acesso as nuvens utilizadas;

2.4.1.6.3. **Serviços fora de escopo**

·Tratamento das vulnerabilidades encontradas nas nuvens do cliente;

·Criação de políticas de segurança para nuvem;

·Administração de infraestrutura de TI: o serviço não contempla configuração de nuvens, servidores ou políticas de acesso.

2.4.1.6.4. **Suporte Técnico**

	Detecção	**Contenção**	**Resposta**
Bronze [N1]	**Até 4 horas**	**Até 8 horas**	**Até 12 horas**
Prata [N2]	**Até 2 horas**	**Até 4 horas**	**Até 8 horas**
Ouro [N3]	**Até 30 minutos**	**Até 1 hora**	**Até 4 horas**

2.4.1.6.5. **Horário de atendimento**

·O atendimento será realizado em regime SOC 24x7, com monitoramento contínuo e resposta imediata a eventos provenientes de vulnerabilidades encontradas na nuvem.

2.4.1.6.6. SLA para Atendimento

24 x 7 x365

2.4.1.7. **WAF**

O recurso de WAF (Web Application Firewall) garante a proteção aplicações web contra-ataques.

Ele analisa o tráfego HTTP/HTTPS em tempo real, filtrando requisições maliciosas antes de chegarem ao servidor.

Bloqueia ameaças como SQL Injection, Cross-Site Scripting (XSS), LFI/RFI e exploração de vulnerabilidades conhecidas.

Pode operar em modo de bloqueio ou apenas de monitoramento, conforme as políticas definidas.

Assim, reduz riscos de indisponibilidade, vazamento de dados e comprometimento das aplicações web.

2.4.1.7.1. **Atividades Previstas**

·Monitoramento contínuo de tráfego HTTP/HTTPS para aplicações web e APIs;

·Detecção e bloqueio de ataques em tempo real com base em regras gerenciadas;

·Criação e ajuste de políticas de segurança automatizadas;

·Proteção contra bots maliciosos e abuso de APIs;

2.4.1.7.2. **Entregáveis**

·Dashboards de tráfego e segurança: indicadores de ameaças, desempenho e eficácia;

·Políticas de segurança personalizadas: iegras adaptadas ao ambiente do cliente;

2.4.1.7.3. **Pré-requisitos**

·Inventário de aplicações e APIs protegidas;

2.4.1.7.4. **Serviço fora do Escopo**

·Desenvolvimento de aplicações ou APIs;

·Remediação de vulnerabilidades em código-fonte;

·Gestão de certificados SSL fora da plataforma;

·Monitoramento de ameaças fora da camada de aplicação (ex: rede, endpoint);

·Auditorias formais e gestão de riscos corporativos;

·Suporte ao usuário final ou help desk;

2.4.1.7.5. **Suporte Técnico**

·O serviço será operado remotamente, com suporte técnico especializado para integração, tuning e análise de eventos relacionados ao WAF.

2.4.1.7.6. **Horário de atendimento**

·O atendimento será realizado em regime SOC 24x7, com monitoramento contínuo e resposta imediata a eventos de segurança na camada de aplicação

2.4.1.7.6. **SLA para Atendimento**

24 x7 x365

SLA	**Detecção**	**Contenção**	**Resposta**
Bronze [N1]	**Até 4 horas**	**Até 8 horas**	**Até 12 horas**
Prata [N2]	**Até 2 horas**	**Até 4 horas**	**Até 8 horas**
Ouro [N3]	**Até 30 minutos**	**Até 1 hora**	**Até 4 horas**

2.4.1.8. Pentest

Os serviços de Pentest (teste de penetração) são simulações controladas de ataque cibernético contra sistemas, redes ou aplicações.

Pode ser conduzido em diferentes abordagens, como Black Box e Grey Box.

Os resultados fornecem relatórios detalhados com falhas, riscos e recomendações de mitigação.

Assim, fortalece a postura de segurança e apoia a conformidade regulatória.

2.4.1.8.1. **Serviços de Red Team**

Serviço composto por avaliações de fragilidades de estruturas tecnológicas via reconhecimento ativo. De forma a mapear vulnerabilidades, pontos de entrada, riscos de exploração e usuários comprometidos. Há possibilidade de atuação via exploração direcionada a usuários, IPs, sites e aplicações.

2.4.1.8.2. **Atividades Previstas**

·Reunião para definição de escopo, alvos e métodos.

·Elaboração de documento de NDA (Non-Disclosure Agreement - Acordo de Não Divulgação) entre as partes;

·Execução do serviço em período de 10 dias;

·Aprofundamento dos casos de exploração;

·Apoio para o desenvolvimento de planos de recuperação de incidentes de segurança;

·Recomendações de melhoria do ambiente, com base nos resultados alcançados.

2.4.1.8.3. **Entregáveis**

·Relatório detalhando a jornada de Red Teaming executada, bem como os findings identificados, métodos de exploração que tiveram sucesso e insucesso, dados identificados, serviços, aplicações e vulnerabilidades (quando identificadas) exploradas e recomendações de melhoria da postura de segurança do ambiente.

2.4.1.8.4. **Pré-requisitos**

·Assinatura de NDA (Non-Disclosure Agreement - Acordo de Não Divulgação) entre as partes;

·Reunião de escopo e definição de alvos;

·Ponto de contato durante execução do serviço de Red Teaming;

2.4.1.8.5. **Suporte Técnico e Monitoramento**

·A disponibilidade do serviço de Red Teaming/Pentest é de 10 dias por cada slot contratado, podendo ser solicitado dentro de 12 meses, a contar da assinatura do presente contrato.

2.4.1.9. **CTI**

CTI (Cyber Threat Intelligence) é um serviço de inteligência em cibersegurança que coleta, analisa e compartilha informações sobre ameaças digitais.

Ele antecipa possíveis ataques identificando táticas, técnicas e procedimentos (TTPs) usados por cibercriminosos.

Permite monitorar fontes abertas, fechadas e deep/dark web para detectar indícios de ataques direcionados.

Gera relatórios acionáveis para apoiar decisões de defesa, resposta a incidentes e gestão de riscos.

Assim, o CTI fortalece a segurança preventiva e aumenta a capacidade de reação das organizações.

2.4.1.9.1. **Atividades Previstas**

·Lista atualizada de ameaças, com países e setores afetados, escopo e data;

·Exibição de perfis de criminosos cibernéticos, incluindo alias, táticas e mais;

·Pesquisa de ameaças com base em CVEs, TTPs, malware, etc., e refina investigações;

·Gestão de exposição a riscos, relacionando CVEs específicas com ameaças emergentes e queries de caça, ajudando a priorizar ações de mitigação;

·Monitoramento e notificação de alertas, bloqueios e comportamentos suspeitos.

2.4.1.9.2. **Entregáveis**

·Relatórios mensais contemplando evidências dos alertas.

2.4.1.9.4. **Suporte Técnico**

·O serviço de suporte técnico será realizado remotamente em regime 24x7.

2.4.1.9.4. **Serviços fora do escopo**

·Desenvolvimento e manutenção de aplicativos e sistemas;

·Suporte aos usuários dos sistemas utilizados pela CONTRATANTE;

2.4.1.10. **Serviços**

As atividades do SOC serão realizadas em colaboração entre a CONTRATADA e a SGGD.

As responsabilidades serão detalhadas no plano de atuação pós-contrato.

O Serviço de monitoramento de incidentes cibernéticos deverá realizar em tempo real, o monitoramento, a análise e o escalonamento de eventos de segurança, garantindo rastreamento contínuo, a emissão de alertas iniciais e o encaminhamento tempestivo às equipes de

“Serviço Pontual de Respostas a Incidentes” ou “Especialistas Integrados à SGGD”, no caso de potenciais incidentes.

·**N1 e N2** - Execução e triagem inicial de eventos com base em playbooks predefinidos, classificando incidentes por criticidade e prioridade, e encaminhando eventos relevantes aos especialistas.

·**Nível 1 (N1)** – Monitoramento e Triagem

o Responsabilidades:

·Monitorar alertas de segurança em tempo real (SIEM, SOAR, EDR, IDS/IPS, Firewalls, etc.).

·Realizar triagem inicial dos eventos para identificar falsos positivos.

·Classificar e priorizar alertas de segurança (baixa, médio e alto);

·Executar procedimentos de resposta automatizados, semiautomatizados ou manuais;

·Abrir tickets, registrar evidências e escalar incidentes quando necessário.

·Enviar alertas qualificados para análise dos Analistas de Segurança nível 2;

·Bloquear usuários, IPs ou hosts conforme regras predefinidas;

·Identificar e sugerir melhorias em procedimentos;

·**Nível 2 (N2)** – Análise Avançada e Contenção

o Responsabilidades:

·Analisar alertas escalonados do N1 com profundidade;

·Correlacionar múltiplos eventos para identificar padrões de ataque.

·Apoiar o time de segurança do cliente na realização de análises forenses iniciais em logs, endpoints e tráfego de rede.

·Apoiar na comunicação com times internos de TI e responsáveis pelos ativos impactados.

·Trabalhar junto com times de infraestrutura, suporte, aplicações e parceiros a fim de investigar causas-raiz;

·Identificar e sugerir melhorias em regras de detecção no SIEM;

·Realizar hunting de ameaças com base em IoCs, táticas MITRE ATT&CK, etc;

·Auxiliar na contenção e erradicação de incidentes de segurança;

·Propor melhorias em processos, regras e playbooks;

·**Nível 3 (N3)** – Especialistas e Threat Hunting

o Responsabilidades:

·Atuar em incidentes críticos ou de alta complexidade (ex.: ransomware, APTs, exfiltração de dados).

·Executar análises forenses completas em sistemas comprometidos.

·Conduzir threat hunting proativo, buscando indícios de ataques que não geraram alertas automatizados.

·Desenvolver e otimizar regras de detecção, casos de uso e playbooks no SIEM/SOAR.

·Interagir com equipes externas (CERTs, órgãos reguladores, autoridades).

·Apoiar em auditorias, relatórios executivos e recomendações estratégicas de segurança.

·Suportar a integração de novas fontes de logs no SIEM;

·Criar casos de uso, regras de correlação, dashboards, documentação e treinamento;

·Conduzir resposta a incidentes críticos (coordenar contenção, análise forense, etc.);

·Produzir relatórios técnicos e executivos de incidentes;

·Investigar incidentes avançados (APT, ransomware, insider threat, etc.);

·Realizar hunting manual baseado em hipóteses ou inteligência externa;

·Comunicação segura e contínua entre as Salas de Monitoramento da CONTRATADA e da SGGD, garantindo alinhamento nas atividades, compartilhamento tempestivo de informações sobre ameaças e integração de dados para análise.

2.5. **SOC Room**

A Sala de Monitoramento de Incidentes Cibernéticos, ou "SOC Room" (Security Operations Center Room), é o epicentro operacional de um SOC. É um ambiente físico ou, em alguns casos, uma estrutura lógica e distribuída, onde equipes especializadas trabalham 24/7 (ou em turnos definidos) para detectar, analisar, investigar e responder a ameaças e incidentes de segurança cibernética em tempo real.

2.5.1. **Componentes Essenciais da Sala de Monitoramento**

2.5.1.1. Pessoas

Analista de segurança, especialistas, e gestores de incidentes, são a primeira linha de defesa e a inteligência por trás das ferramentas. Eles utilizam as plataformas tecnológicas para:

·Monitoramento Contínuo: Observam alertas e dashboards.

·Análise de Eventos: Investigam a relevância e o potencial impacto de cada alerta.

·Caça a Ameaças (Threat Hunting): Proativamente buscam por atividades maliciosas que as ferramentas automáticas possam ter perdido.

·Resposta a Incidentes: Executam planos de contenção, erradicação e recuperação.

2.5.1.2. **Tecnologia**

O fornecendo de soluções de ponta que são a espinha dorsal de qualquer SOC moderno conforme descrito nos demais itens desta especificação de serviços.

Plataforma de monitoramento para monitorar e otimizar o desempenho de aplicativos e infraestrutura de TI onde deverá conter minimamente as seguintes especificações:

·1 painel de VideoWall 4×2 formando tela única **de mínimo 4,30m x 1,20m**.

·4 monitores profissionais de **49"**, novos e sem uso anterior.

·Proporção de tela **16:9**, tecnologia **IPS**.

·Borda ultrafina: **máximo 3,5mm** na junção das telas.

·Brilho mínimo: **450 cd/m²**.

·Conectividade:

·**INPUT:** HDMI, DP, DVI-D, AUDIO, USB 2.0.

·**OUTPUT:** DP, AUDIO.

·Autoajuste de brilho e contraste na junção das telas.

·Alimentação**: AC 100-240V 50/60Hz**.

·Cabos para conexão entre unidades.

·Compatível com o modelo de monitor ofertado.

·Suporte fixo com ajustes de nível e profundidade.

·Fabricado em **aço carbono** com pintura **Epóxi de alta resistência**.

·Possuir **travamento de segurança.**

·Instalação na sala de monitoramento **NOC.**

2.5.1.3. **Processos**

·Planos de Resposta a Incidentes (IRP): Documentos detalhados sobre como responder a diferentes tipos de ataques.

·Playbooks: Roteiros passo a passo para as tarefas de resposta a incidentes, muitas vezes automatizados pelo SOAR.

·Runbooks: Procedimentos operacionais padrão para tarefas rotineiras de segurança.

·KPIs e Métricas: Medir a eficácia do SOC, como tempo médio de detecção (MTTD) e tempo médio de resposta (MTTR).

2.6. **Serviço Pontual de Resposta a Incidentes**

·Serão destacadas as características esperadas e os quantitativos estimados para atendimento de demandas pontuais de resposta a incidentes.

3. **PRAZOS**

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

4. **RESPONSABILIDADES DAS PARTES**

Além das obrigações constantes da Cláusula – "OBRIGAÇÕES DAS PARTES" do contrato a que se vincula esta ESP, ficam definidas as enunciadas a seguir:

4.1. **DA CONTRATADA**

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

3.1.2. Manter sigilo de todas as informações coletadas nos sistemas legado, servidores;

3.1.3. Comunicar imediatamente à CONTRATANTE qualquer evento relativo aos serviços definidos nesta ESP;

4.2. **DA CONTRATANTE**

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

3.2.2. Para cada serviço administrado, indicar um contato para esclarecimento de dúvidas ou procedimentos;

3.2.3. Informar a disponibilidade dos aplicativos, as informações técnicas e a periodicidade dos serviços para a realização das atividades;

3.2.4. Realizar configurações e liberações de acesso para a realização das atividades quando necessário;

3.2.5. Disponibilizar um local e uma estação de trabalho nas localidades das atividades quando necessário.

5. **PREÇO E CONDIÇÕES DE PAGAMENTO**

O preço para a execução dos serviços constantes desta ESP é estimado em **R$ 62.652.009,24** (**Sessenta e dois milhões, seiscentos e cinquenta e dois mil, nove reais e vinte e quatro centavos**), tendo como data base de referência o **OUTUBRO/2025** e será reajustado de acordo com as condições estabelecidas no contrato a que se vincula.

ITEM	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	QTDE PREVISTA		VALOR UNITÁRIO	QTDE MESES	VALOR PREVISTO	
			QTDE MÊS	QTDE TOTAL			PARCELA MENSAL	TOTAL
5.1	**Paas Middleware**						**R$ 4.784.065,32**	**R$ 57.408.783,84**
5.1.1	Pass Middleware	UNIDADE DE MIDDLEWARE / MÊS	2829	33948	R$ 1.691,08	12	R$ 4.784.065,32	R$ 57.408.783,84
5.2	**Gestão**						**R$ 436.935,45**	**R$ 5.243.225,40**
5.2.1	Serviço de Gestão de Operações Prata	POR UNIDADE DE GESTÃO / MÊS	1	12	R$ 84.733,05	12	R$ 84.733,05	R$ 1.016.796,60

5.2.2	Serviço de Gestão de Operações Ouro	POR UNIDADE DE GESTÃO / MÊS	2	24	R$ 176.101,20	12	R$ 352.202,40	R$ 4.226.428,80
TOTAL							**R$ 5.221.000,77**	**R$ 62.652.009,24**

Os subitens serão faturados da seguinte forma:

·Todos os subitens serão pagos em parcela fixa mensal;

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

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

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

6. VIGÊNCIA DO DOCUMENTO

A ESP terá vigência de **12 (doze)** meses a partir da data da assinatura do Contrato.

7. VALIDADE DOS PREÇOS

Os preços constantes desta ESP são válidos (30) dias por após a data de sua emissão.

·24 x7 x 365

2.2.1.6. SLA para Atendimento:

·Gestão da alocação dos profissionais, se previstos no projeto;

Tal visão granular potencializa a visão dos riscos que possam elevar a fragilidade do ambiente frente a ataques cibernéticos e que afetem disponibilidade dos serviços e operação. Ainda, promove visão das vulnerabilidades existentes nas estações de trabalho, servidores e ambientes em nuvem. Junto ao mapeamento de riscos focados em estruturas de cloud pública e híbrida como AWS, GCP, Azure e OCI, de forma a identificar riscos intrínsecos em configurações, acessos e recursos que possam ser uma porta entrada para um ataque ou uma fragilidade exposta passível de ser explorada. Portanto, cada pilar contribui para o mapeamento da superfície de ataque do ambiente, de forma a mapear os riscos existentes e traçar ações de redução.

·Sistema Operacional:

o Windows 10 22H2 (32bit e 64bit);

o Windows 11 (32bit e 64bit);

o Windows Server 2008 R2 (64bit) ou superior;

o CentOS 6 (64bit) ou superior;

o Debian 10 ou superior (64bit);

o Ubuntu 16.04 (64bit) ou superior;

o Amazon Linux 2 ou superior (64bit);

o Oracle Linux 7 (64bit) ou superior;

o RHEL 6 (64bit) ou superior;

·Processador:

o Mínimo 2.0 GHz Intel Pentium ou equivalente (4-core);

·Memória (RAM):

o Mínimo de 3GB exclusivamente para o agente da solução em desktops;

·Espaço de disco:

o Mínimo de 5GB

2.4.1.1.4. **Suporte Técnico**

·O serviço de suporte técnico será realizado remotamente em regime 24x7

2.4.1.1.5. **Horário de Atendimento**

·O atendimento será realizado em regime SOC 24x7, com monitoramento contínuo e resposta conforme SLA para Atendimento detalhado neste documento.

2.4.1.1.6. **SLA para Atendimento:**

24 x7 x365

·Virtualizador VMware ou HyperV.

2.4.1.2.4. **Suporte Técnico**

·O serviço de suporte técnico será realizado remotamente em regime 24x7.

2.4.1.2.5. **Horário de Atendimento**

·O atendimento será realizado em regime SOC 24x7, com monitoramento contínuo e resposta conforme SLA detalhado abaixo.

2.4.1.2.6. **SLA para Atendimento**

·24 x7 x 365

2.4.1.3. **EPM em Servidores**

·Proteção contra ameaças de Pass-The-Hash (roubo de um hash de senha que pode ser utilizado para mover lateralmente na rede);

2.4.1.4.6. **Horário de Atendimento**

·O atendimento será realizado em regime SOC 24x7, com monitoramento contínuo e resposta imediata a eventos de ransomware.

2.4.1.4.7. SLA para atendimento

24 x7 x365

·Dashboards customizados com evidências para auditorias.

·O serviço será operado remotamente, com suporte técnico especializado para integração, tuning e análise de eventos relacionados ao fabricante.

·Relatórios mensais de eventos bloqueados: detalhamento de ataques detectados e mitigados;

Seu objetivo é identificar vulnerabilidades exploráveis antes que criminosos as utilizem.

·Gerenciamento, monitoramento, manutenção e suporte à infraestrutura e aos usuários locais no ambiente de TIC.

·Apoiar o time de segurança do cliente em ações de contenção mais complexas, como quarentena de sistemas, segmentação de rede, aplicação de patches emergenciais.

·Analisar vulnerabilidades e apoiar o time de hardening/patching;

·Resolução mínima: **1920 x 1080 pixels (Full HD)**.

8. CONTATO NA PRODESP

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

ÁREA DE NEGÓCIOS

Nome : Selma Berezutchi Aftim

Endereço: Rua Agueda Gonçalves, 240 - 2º andar - Taboão da Serra - SP Telefone : (011) 2868-3124

E-mail : saftim@sp.gov.br

ÁREA RESPONSÁVEL PELA EXECUÇÃO DO SERVIÇO

Nome : Jobson Nunes de Souza

Endereço : Rua Agueda Gonçalves, 240 – Mezanino (Cúpula) – Jardim Pedro Gonçalves - Taboão da Serra – SP.

Telefone : (11) 2845-6344

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

ANEXO III - PRÁTICAS PROIBIDAS

Práticas Proibidas

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

(a) O Banco define, para os fins desta disposição, os seguintes termos:

(i) uma prática corrupta consiste em oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer coisa de valor para influenciar indevidamente as ações de outra parte;

(ii) uma prática fraudulenta é qualquer ato ou omissão, incluindo a tergiversação de fatos ou circunstâncias que deliberada ou imprudentemente engane ou tente enganar, uma parte para obter um benefício financeiro ou de outra natureza ou para evitar cumprir uma obrigação;

(iii) uma prática coercitiva consiste em prejudicar ou causar dano, ou ameaçar prejudicar ou causar dano, direta ou indiretamente, a qualquer parte interessada ou à sua propriedade, para influenciar indevidamente as ações de uma parte;

(iv) uma prática colusiva é um acordo entre duas ou mais partes com o intuito de alcançar um propósito impróprio, inclusive influenciar inapropriadamente as ações de outra parte;

(v) Uma prática obstrutiva é:

i. destruir, falsificar, alterar ou ocultar evidências significativas de uma investigação do Grupo BID ou prestar declarações falsas aos investigadores com a intenção de obstruir uma investigação do Grupo BID;

ii. ameaçar, assediar ou intimidar qualquer parte interessada para impedi-la de revelar seu conhecimento sobre assuntos relevantes para uma investigação do Grupo BID ou ao seu prosseguimento; ou

iii. atos que visem impedir o exercício dos direitos contratuais de auditoria ou inspeção do Grupo BID previstos nas IAL 1.1 (f) abaixo ou seus direitos de acesso à informação; e

(vi) uma apropriação indébita consiste no uso de fundos ou recursos do Grupo BID para um propósito impróprio ou não autorizado, cometido

intencionalmente ou por negligência grave.

(b) Se o Banco determinar que em qualquer estágio da aquisição ou da execução de um contrato qualquer empresa, entidade ou indivíduo que concorra ou participe de uma atividade financiada pelo Banco, incluindo, entre outros, requerentes, licitantes, proponentes, fornecedores de bens, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços, concessionários, Mutuários (incluindo Beneficiários de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos dirigentes, funcionários e agentes, independentemente de a agência ser expressa ou implícita) envolvidos em uma Prática Proibida, o Banco poderá:

(i) não financiar nenhuma recomendação de adjudicação de um contrato para obras, bens e serviços correlatos financiados pelo Banco;

(ii) suspender os desembolsos da operação se for determinado, em qualquer etapa, que um funcionário, agente ou representante do Mutuário, da Agência Executora ou Agência Contratante se envolveu em Prática Proibida;

(iii) declarar a Aquisição Viciada (Misprocurement) e cancelar e/ou declarar vencido antecipadamente o pagamento da parte do empréstimo ou da doação destinada a um contrato, quando houver evidências de que o representante do Mutuário ou do Beneficiário de uma doação não tomou as medidas corretivas adequadas (incluindo, entre outras, fornecer a notificação adequada ao Banco após tomar conhecimento da Prática Proibida) dentro de um prazo que o Banco considere razoável; (iv) emitir uma advertência à empresa, entidade ou indivíduo através de uma carta formal de censura por sua conduta;

(v) declarar que uma empresa, entidade ou indivíduo é inelegível, permanentemente ou por um prazo determinado, para: (i) receber ou participar em atividades financiadas pelo Banco; e (ii) ser designado[2] como subconsultor, subempreiteiro, fornecedor de bens ou prestador de serviços de uma empresa elegível à qual tenha sido adjudicado um contrato financiado pelo Banco;

(vi) encaminhar o assunto às autoridades competentes, encarregadas de fazer cumprir as leis; e/ou

(vii) impor outras sanções que julgar apropriadas sob as circunstâncias, incluindo a imposição de multas que representem o reembolso do Banco pelos custos associados às investigações e procedimentos. Essas sanções podem ser impostas adicionalmente ou em substituição às sanções mencionadas acima.

(c) As disposições dos incisos (i) e (ii) das IAL 1.1 (b) serão aplicadas, também, quando tais partes tiverem sido temporariamente declaradas inelegíveis para a adjudicação de novos contratos, enquanto aguardam a decisão definitiva de um processo de sanção ou de qualquer outra resolução.

(d) A imposição de qualquer ação a ser tomada pelo Banco de acordo com as disposições acima mencionadas, será pública.

(e) Além disso, qualquer empresa, entidade ou indivíduo que concorra ou participe de uma atividade financiada pelo Banco incluindo, entre outros, requerentes, licitantes, proponentes, fornecedores de bens, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços, concessionários, Mutuários (incluindo Beneficiários de doações), Agências Executoras ou Agências Contratante (incluindo seus respectivos dirigentes, funcionários e agentes, independentemente de a agência ser expressa ou implícita), podem estar sujeitos a sanções baseadas nos acordos que o Banco possa ter com outras IFIs em relação ao reconhecimento mútuo de decisões de exclusão. Para fins deste parágrafo, o termo "sanção" incluirá qualquer exclusão, condições sobre futuras contratações ou qualquer ação divulgada publicamente em resposta a uma violação da estrutura aplicável de uma IFI para tratar de alegações de Práticas Proibidas.

(f) O Banco exige que seja incluída uma disposição nos documentos de licitação e nos contratos financiados com um empréstimo ou doação do Banco, exigindo que os requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços e concessionários, permitam que o Banco inspecione todas e quaisquer contas, registros e outros documentos relativos à apresentação de ofertas e execução de contrato bem como que sejam auditados por auditores nomeados pelo Banco. No âmbito desta política, os requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços e concessionários devem prestar plena assistência ao Banco em sua investigação. O Banco terá também o direito de requerer que, nos contratos por ele financiados com um empréstimo ou doação incluam uma disposição que obrigue os requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, funcionários, subempreiteiros, subconsultores, prestadores de serviços e concessionários a: (i) mantenham todos os documentos e registros referentes às atividades financiadas pelo Banco por sete (7) anos após a conclusão do trabalho contemplado no respectivo contrato; e (ii) forneçam quaisquer documentos necessários à investigação de alegações de Práticas Proibidas; e assegurem que funcionários ou agentes dos requerentes, licitantes, proponentes, fornecedores de bens e seus agentes, empreiteiros, consultores, subempreiteiros, subconsultores, prestadores de serviços ou concessionários que tenham conhecimento das atividades financiadas pelo Banco estejam disponíveis para responder às questões dos funcionários do Banco ou de qualquer investigador, agente, auditor ou consultor relacionado com a investigação devidamente designado. Caso o requerente, licitante, proponente, fornecedor de bens e seus agentes, empreiteiro, consultor, funcionários, subempreiteiro, subconsultor, prestador de serviços ou concessionário se recusem a cooperar e/ou descumpram o exigido pelo Banco ou obstruam de qualquer forma, a investigação, o Banco, a seu critério exclusivo, pode tomar as medidas apropriadas contra o requerente, licitante, proponente, fornecedor de bens e seus agentes, empreiteiro, consultor, funcionários, subempreiteiro, subconsultor, prestador de serviços ou concessionário.

(g) O Banco exigirá que, quando um Mutuário selecionar uma agência especializada para fornecer serviços de assistência técnica, todas as disposições relacionadas às Práticas Proibidas e as sanções correspondentes, serão aplicadas integralmente aos requerentes, licitantes, proponentes, empreiteiros, empresas de consultoria e consultores individuais, funcionários, subempreiteiros, subconsultores, prestadores de serviços ou fornecedores de bens, (incluindo seus respectivos dirigentes, funcionários e agentes, independentemente de a agência ser expressa ou implícita), ou qualquer outra entidade que tenha assinado contratos com essa agência especializada para fornecer bens ou prestar serviços correlatos relacionados com as atividades financiadas pelo Banco. O Banco mantém o direito de exigir que o Mutuário invoque recursos tais como suspensão ou extinção. As agências especializadas deverão consultar a lista do Banco de empresas e indivíduos suspensos ou excluídos. No caso de uma agência especializada assinar um contrato ou uma ordem de compra com uma empresa ou com um indivíduo suspenso ou excluído pelo Banco, o Banco não financiará as despesas relacionadas e aplicará outras medidas conforme apropriado.

1.2 Com a concordância específica do Banco, além da Lista do Banco de Empresas e Indivíduos Sancionados, o Mutuário pode introduzir, nos formulários da Oferta e para contratos financiados pelo Banco, um compromisso do Licitante de observar, ao concorrer e executar um contrato, as leis e o sistema de sanções do país contra Práticas Proibidas (incluindo suborno) e os regulamentos e sanções de um organismo de desenvolvimento multilateral/bilateral ou organização internacional, atuando como cofinanciador, relacionados a práticas proibidas, se aplicável, conforme listado nos documentos de licitação[3]. O Banco aceitará a introdução de tal compromisso a pedido do país Mutuário, desde que as disposições que regem tal requisito sejam satisfatórias para o Banco).

PAÍSES ELEGÍVEIS

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

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

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

---

1) Países-membros quando a fonte de financiamento é o Banco Interamericano de Desenvolvimento:

Alemanha, Argentina, Áustria, Bahamas, Barbados, Bélgica, Belize, Bolívia, Brasil, Canadá, Chile, Colômbia, Costa Rica, Croácia, Dinamarca, Equador, El Salvador, Eslovênia, Espanha, Estados Unidos, Finlândia, França, Guatemala, Guiana, Haiti, Honduras, Israel, Itália, Jamaica, Japão, México, Nicarágua, Noruega, Países Baixos, Panamá, Paraguai, Peru, Portugal, Reino Unido, República da Coreia, República Dominicana, República Popular da China, Suécia, Suíça, Suriname, Trinidade e Tobago, Uruguai, e Venezuela.

Territórios elegíveis

(a) Guadalupe, Guiana Francesa, Martinica, Reunião – por ser Departamentos da França.

(b) Ilhas Virgens dos EUA, Porto Rico, Guam - como Território dos Estados Unidos da América

(c) Aruba - como país constituinte do Reino dos Países Baixos; e Bonaire, Curaçao, Sint Maarten, Sint Eustatius - por serem Departamentos do Reino dos Países Baixos.

(d) Hong Kong - por ser uma Região Administrativa Especial da República Popular da China.

---

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

Brasil

---

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

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

(A) Nacionalidade

(a) Um indivíduo é considerado nacional de um país-membro do Banco se satisfaz um dos seguintes requisitos:

(i) é cidadão de um país-membro; ou

(ii) estabeleceu seu domicílio em um país-membro como residente de “boa-fé” e está legalmente autorizado para trabalhar nesse país.

(b) Uma empresa tem a nacionalidade de um país-membro se satisfizer os dois requisitos a seguir:

(i) está legalmente constituída ou estabelecida conforme as leis de um país-membro do Banco; e

(ii) mais de cinquenta por cento (50%) do capital da empresa é de propriedade de indivíduos ou empresas de países-membros do Banco.

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

(B) Origem dos Bens

Os bens têm origem em um país-membro do Banco se foram extraídos, cultivados, colhidos ou produzidos em um país-membro do Banco. Considera-se que um bem é produzido quando, mediante manufatura, processamento ou montagem, o resultado é um artigo comercialmente reconhecido cujas características, funções ou finalidades de uso são substancialmente diferentes de suas partes ou componentes.

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

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

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

(C) Origem dos Serviços

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

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

[2] Um subconsultor, subempreiteiro, fornecedor de bens ou prestador de serviços nomeado (nomes diferentes podem ser utilizados dependendo do documento de licitação específico) é aquele que: (i) foi indicado pelo licitante em sua pré-qualificação ou oferta porque traz

experiência e know-how específicos e cruciais que permitem ao licitante atender às exigências de qualificação para a licitação em questão; ou (ii) foi indicado pelo Mutuário.

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

Documento assinado eletronicamente por **Otilia Carla dos Santos**, **Chefe de Assessoria**, em 26/12/2025, às 17:43, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thiago Waltz**, **Diretor**, em 29/12/2025, às 10:40, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Gileno Gurjao Barreto**, **Diretor Presidente**, em 29/12/2025, às 12:19, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Alyne Lima Rodrigues**, **Assessor Especial I**, em 29/12/2025, às 18:03, 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 **0093324477** e o código CRC **99CF082C**.

Governo do Estado de São Paulo
Secretaria de Gestão e Governo Digital
Divisão de Contratos

TERMO DE CIÊNCIA DE NOTIFICAÇÃO

CONTRATANTE: SECRETARIA DE GESTÃO E GOVERNO DIGITAL

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

CONTRATO Nº 084/2025

OBJETO: CONTRATAÇÃO DE CENTRO DE OPERAÇÕES DE SEGURANÇA (SECURITY OPERATIONS CENTER)

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 do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, 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 pelacontratante e interessados estão cadastradas no módulo eletrônico do “Cadastro Corporativo TCESP – CadTCESP”, nos termos previstos no Artigo 2º das Instruções nº01/2020, 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.

São Paulo/SP, na data da assinatura digital

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:
Nome: CAIO MÁRIO PAES DE ANDRADE
Cargo: Secretário de Gestão e Governo Digital
CPF: 326.865.105-44

RESPONSÁVEL PELA AUTORIZAÇÃO:
Nome: DIEGO CÉSAR SANTANA MENDES
Cargo: Diretor
CPF: 741.728.401-91
Assinatura: assinado digitalmente

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:

Pelo contratante:
Nome: OTILIA CARLA DOS SANTOS
Cargo: Chefe de Assessoria
CPF: 293.377.078-45
Assinatura: assinado digitalmente

Pela contratada:
Nome: THIAGO WALTZ ALVES
Cargo: Diretor de Relacionamento com Clientes
CPF: 950.082.761-15
Assinatura: assinado digitalmente

Pela contratada:
Nome: GILENO GURJÃO BARRETO
Cargo: Diretor-Presidente
CPF:315.099.595-72
Assinatura: assinado digitalmente

ORDENADOR DE DESPESAS DA CONTRATANTE:
Nome: OTILIA CARLA DOS SANTOS
Cargo: Chefe de Assessoria
CPF: 293.377.078-45

Assinatura: assinado digitalmente

GESTORA:
Nome: ALYNE LIMA RODRIGUES
Cargo: Diretora
CPF: 321.312.688-82
Assinatura: assinado digitalmente

GESTOR SUBSTITUTO:
Nome: DENIS ALVES RODRIGUES
Cargo: Diretor
CPF: 290.215.188-80
Assinatura: assinado digitalmente

FISCAL TÉCNICO:
Nome: JUAN ZAMARRENHO CARVALHO CORRÊA
Cargo: Coordenador
CPF: 481.882.328-74
Assinatura: assinado digitalmente

FISCAL TÉCNICO SUBSTITUTO:
Nome: CINTYA TAKAHASCHI
Cargo: Coordenadora
CPF: 178.508.538-73
Assinatura: assinado digitalmente

FISCAL ADMINISTRATIVO:
Nome: THAIS PRISCILA DE SOUSA E SILVA DEPIERI
Cargo: Assessora IV
CPF: 125.900.488-07
Assinatura: assinado digitalmente

(*) - O Termo de Ciência e Notificação e/ou Cadastro do(s) Responsável(is) deve identificar as pessoas físicas que tenham concorrido para a prática do ato jurídico, na condição de ordenador da despesa; de partes contratantes; de responsáveis por ações de acompanhamento, monitoramento e avaliação; de responsáveis por processos licitatórios; de responsáveis por prestações de contas; de responsáveis com atribuições previstas em atos legais ou administrativos e de interessados relacionados a processos de competência deste Tribunal.Na hipótese de prestações de contas, caso o signatário do parecer conclusivo seja distinto daqueles já arrolados como subscritores do Termo de Ciência e Notificação, será ele objeto de notificação específica. (inciso acrescido pela Resolução nº 11/2021)

Documento assinado eletronicamente por **Otilia Carla dos Santos**, **Chefe de Assessoria**, em 26/12/2025, às 17:21, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thais Priscila De Sousa E Silva Depieri**, **Assessor IV**, em 29/12/2025, às 08:34, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Thiago Waltz**, **Diretor**, em 29/12/2025, às 10:40, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Cintya Takahaschi**, **Coordenador**, em 29/12/2025, às 12:51, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Juan Zamarrenho Carvalho Correa**, **Coordenador**, em 29/12/2025, às 14:45, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Alyne Lima Rodrigues**, **Assessor Especial I**, em 29/12/2025, às 17:44, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Gileno Gurjao Barreto**, **Diretor Presidente**, em 29/12/2025, às 18:48, 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 **0093334080** e o código CRC **77D961D8**.

ANEXO I
PLANILHA DE ORÇAMENTO
ESPECIFICAÇÃO DE SERVIÇOS E PREÇOS [E0250354]
CONTRATO [PD025290]
SGGD - SOC

ITEM	DENOMINAÇÃO DOS SERVIÇOS	UNIDADE DE MEDIDA	QTDE PREVISTA		VALOR UNITÁRIO	QTDE MESES	VALOR PREVISTO	
			QTDE MÊS	QTDE TOTAL			PARCELA MENSAL	TOTAL
5.1	**Paas Middleware**						**R$ 4.784.065,32**	**R$ 57.408.783,84**
5.1.1	Pass Middleware	UNIDADE DE MIDDLEWARE / MÊS	2829	33948	R$ 1.691,08	12	R$ 4.784.065,32	R$ 57.408.783,84
5.2	**Gestão**						**R$ 436.935,45**	**R$ 5.243.225,40**
5.2.1	Serviço de Gestão de Operações Prata	POR UNIDADE DE GESTÃO / MÊS	1	12	R$ 84.733,05	12	R$ 84.733,05	R$ 1.016.796,60
5.2.2	Serviço de Gestão de Operações Ouro	POR UNIDADE DE GESTÃO / MÊS	2	24	R$ 176.101,20	12	R$ 352.202,40	R$ 4.226.428,80
TOTAL							**R$ 5.221.000,77**	**R$ 62.652.009,24**