CIDADE DE SÃO PAULO
FAZENDA

COMISSÃO PERMANENTE DE LICITAÇÕES – CPL
Lei Federal nº 14.133/2021 e Decreto Municipal 62.100/2022
EDITAL DO PREGÃO ELETRÔNICO SF Nº 17/2023

PROCESSO ELETRÔNICO Nº. 6017.2023/0033846-3

TIPO DE LICITAÇÃO: MENOR PREÇO TOTAL

MODO DE DISPUTA: ABERTO E FECHADO

OBJETO: Contratação de serviços de Segurança da Informação (SOC – Security Operations Center), pelo período de 36 meses, conforme condições e exigências estabelecidas no Termo de Referência – Anexo II.

ENDEREÇO ELETRÔNICO: https://www.gov.br/compras

UASG 925011 – PMSP – Secretaria Municipal da Fazenda

DATA E HORA DA ABERTURA DA SESSÃO PÚBLICA: 04/12/2023 às 10h00

EXCLUSIVO PARA ME/EPP/EQUIPARADAS: NÃO

FASE DE HABILITAÇÃO: Após as fases de apresentação de propostas, lances e julgamento.

ÍNDICE

CIDADE DE SÃO PAULO
FAZENDA

PREÂMBULO

A PREFEITURA DO MUNICÍPIO DE SÃO PAULO, pela **Comissão Permanente de Licitações da Secretaria Municipal da Fazenda,** situada na Rua Líbero Badaró, nº 190 – 17º andar – Centro, São Paulo/ SP, Capital, CEP: 01008-000, torna público, para conhecimento de quantos possam se interessar, que fará realizar licitação na modalidade **PREGÃO ELETRONICO**, com critério de julgamento de **MENOR PREÇO TOTAL**, objetivando a prestação do serviço descrito na Cláusula 2 – DO OBJETO deste Edital.

A participação no presente pregão dar-se-á por meio de sistema eletrônico, **pelo acesso ao site** https://www.gov.br/compras, - UASG nº 925011**,** nas condições descritas neste Edital, devendo ser observado o início da sessão às **10h00 do dia 04/12/2023.**

Este Edital, seus anexos, o resultado do Pregão e os demais atos pertinentes também constarão do site http://e-negocioscidadesp.prefeitura.sp.gov.br – Secretaria Municipal da Fazenda.

1. EMBASAMENTO LEGAL

1.1. O procedimento licitatório e os atos dele decorrentes observarão as disposições da Lei Federal nº 14.133/21, do Decreto Municipal nº 62.100/2022, Decreto Municipal nº 56.475/2015 e da Complementar nº 123/2006, alterada pela Lei Complementar nº 147/2014, e das demais normas complementares aplicáveis.

2. OBJETO

2.1. O presente pregão tem por objeto a contratação de serviços de Segurança da Informação (SOC – Security Operations Center), pelo período de 36 meses, nos termos da tabela abaixo, conforme condições e exigências estabelecidas no Termo de Referência – Anexo II.

ITEM	**1. Serviço de gestão de vulnerabilidades**		
1	**Especificação**	**Medição**	**Qtde Mensal**
	Aplicações Web	URL	154
	Ativos de Rede	Ips/Dispositivos	2.208
	Containers	Imagem de Container	130
ITEM	**2. Serviço de monitoramento de ataques cibernéticos**		
2	**Tipo**	**Medição**	**Qtde Mensal**
	Correlacionamento de pacotes	EPS	4.000
	Detecção e resposta em Endpoint	Dispositivo	2.059
ITEM	**3. Serviço de respostas aos incidentes de segurança e de privacidade**		
3	**Tipo**	**Medição**	**Qtde Mensal**
	Resposta Incidentes	Valor Mensal	1
ITEM	**4. Serviço de inteligência aplicado à segurança**		
4	**Tipo**	**Medição**	**Qtde Mensal**
	Monitoramento	Valor Mensal	1
ITEM	**5. Serviços de Teste de Invasão**		
5	**Tipo**	**Medição**	**Qtde Mensal**
	Reserva de Horas	Hora Homem	50
ITEM	**6. Serviços técnicos especializados**		
6	**Tipo**	**Medição**	**Qtde Mensal**
	Reserva de Horas	Hora Homem	50

3. CONDIÇÕES DE PARTICIPAÇÃO

3.1. Poderão participar da licitação as empresas que:

a) atenderem a todas as exigências deste edital e de seus anexos, desde que sejam credenciadas, com cadastro ativo, no Sistema de Cadastramento Unificado de Fornecedores – SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras) – Certificado Digital ICP-Brasil.

a.1) As condições de cadastramento no SICAF deverão ser providenciadas até o terceiro dia útil anterior à data estabelecida para recebimento das propostas.

b) tenham objeto social pertinente e compatível ao licitado;

c) não estejam sob processo de falência;

c.1) Nos termos do artigo 52, inciso I da Lei Federal nº 11.101/05 e da decisão do E. Superior Tribunal de Justiça no Agravo de Instrumento Especial nº 309.867- ES (2013/0064947-3 – Rel. Min. Gurgel de Faria) poderão participar desta licitação as empresas em recuperação judicial ou extrajudicial, desde que demonstrem, na fase de habilitação, sua viabilidade econômica;

d) empresas constituídas em forma de consórcio (art. 15 da Lei 14.133/2021);

e) não tenham sido declaradas inidôneas para licitar e contratar com a Administração Pública;

f) não estejam suspensas ou impedidas de licitar e contratar com a Administração Pública, nos termos da Orientação Normativa PGM 03/2012 e jurisprudência consolidada do Superior Tribunal de Justiça;

g) não se enquadrem nas seguintes vedações de participação (art. 14 da Lei 14.133/2021):

g.1) pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta, estendendo-se a vedação ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que comprovado o ilícito ou utilização fraudulenta da personalidade jurídica do licitante;

g.2) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação 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, devendo essa proibição constar expressamente do edital de licitação;

g.3) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

g.4) Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público de órgão ou entidade licitante ou contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria;

g.4.1) As vedações estendem-se a 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.

g.5) Não poderão participar da licitação OSCIP's atuando nessa condição.

3.2. As **MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE**, assim qualificadas nos termos da Lei Complementar 123/06, alterada pela Lei Complementar 147/2014, bem como as **COOPERATIVAS** que preencham as condições estabelecidas no artigo 1º, §2º, do Decreto nº 56.475/2015, poderão participar desta licitação usufruindo dos benefícios estabelecidos nos artigos 42 a 45 daquela Lei Complementar, devendo para tanto observar as regras estabelecidas de acordo com o Decreto nº 56.475/2015, declarando no campo próprio do sistema sua condição.

3.2.1. Não são aplicáveis os benefícios e demais disposições previstas nos artigos 42 a 49 da Lei Complementar 147/2014 no caso de licitação para aquisição de bens ou contratação de serviços em geral, ao item e, em se tratando de contratação de obras e serviços de engenharia, às licitações cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

3.2.1.1. A obtenção dos benefícios fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

3.2.1.2. Nas contratações com prazo de vigência superior a 1 (um) ano, será considerado o valor anual do contrato.

3.3. Como requisito para a participação no pregão, a licitante deverá declarar, em campo próprio do sistema eletrônico, que está ciente e concorda com as condições do edital e anexos.

3.4. A participação neste Pregão implica o reconhecimento pela Licitante de que conhece, atende e se submete a todas as cláusulas e condições do presente edital, bem como as disposições contidas na legislação indicada na cláusula "1" deste Edital, que disciplinam a presente licitação e integrarão o ajuste correspondente, no que lhe for pertinente.

4. ACESSO ÀS INFORMAÇÕES

4.1. Qualquer pessoa poderá solicitar **ESCLARECIMENTOS** ou **INFORMAÇÕES** relativas a esta licitação, que serão prestados mediante solicitação dirigida ao Pregoeiro, até 03 (três) dias úteis antes da data marcada para abertura do certame, por meio do endereço eletrônico cpl@sf.prefeitura.sp.gov.br, com cópia para fabianaoliveira@sf.prefeitura.sp.gov.br.

4.2. Os esclarecimentos e as informações serão prestados no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data de abertura do certame.

5. IMPUGNAÇÃO AO EDITAL

5.1. Qualquer pessoa, física ou jurídica poderá formular **IMPUGNAÇÕES** contra o ato convocatório, até 3 (três) dias úteis antes da data marcada para abertura do certame, mediante petição apresentada via e-mail, eletrônico cpl@sf.prefeitura.sp.gov.br, com cópia para fabianaoliveira@sf.prefeitura.sp.gov.br, em seu corpo ou documento anexo.

5.2. No ato da apresentação da impugnação **é obrigatório anexar ao e-mail** a cópia digitalizada dos seguintes documentos:

a) do documento de identidade e do Cadastro de Pessoas Físicas (CPF), se o impugnante for pessoa física;

b) do Cadastro Nacional de Pessoas Jurídicas (CNPJ), em se tratando de pessoa jurídica, acompanhado do respectivo ato constitutivo ou de procuração, que comprove que o signatário/remetente da impugnação efetivamente representa a impugnante.

5.3. Caberá ao agente de contratação se manifestar, motivadamente, a respeito da(s) impugnação(ões), proferindo sua decisão no prazo de 03 (três) dias úteis, contados da data de recebimento, limitado ao último dia útil anterior à data da abertura do certame

5.4. Quando o acolhimento da impugnação implicar alteração do edital capaz de afetar a formulação das propostas, será designada nova data para a realização do certame.

5.5. A decisão sobre a impugnação será publicada no sítio eletrônico oficial.

5.6. Os pedidos de impugnações, bem como as respectivas respostas serão divulgados no sistema eletrônico para visualização dos interessados.

5.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

5.8. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

6. APRESENTAÇÃO DA PROPOSTA DE PREÇOS

6.1. Os licitantes encaminharão, **exclusivamente por meio do sistema**, a proposta com a descrição do objeto e o preço ou percentual de desconto, com o **VALOR DO PREÇO TOTAL**, com duas casas decimais, até a data e o horário estabelecidos para a abertura da sessão pública, devendo, no cadastramento da proposta, proceder às declarações pertinentes, em campo próprio do sistema.

6.1.1. O valor a ser lançado no sistema corresponde ao valor total da proposta de preços para os serviços pelo período de 36 meses.

6.2. Até a abertura da sessão, a licitante poderá retirar ou substituir a proposta anteriormente apresentada.

6.3. A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiros sua proposta, lances e declarações.

6.4. A apresentação da proposta de preços implicará em plena aceitação, por parte da licitante, das condições estabelecidas neste Edital e em seus anexos.

6.5. A proposta deve conter oferta firme e precisa, sem alternativa de produtos, preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado.

6.6. Os preços cotados deverão ser cotados em moeda corrente nacional, em algarismos e devem ser adequados aos praticados no mercado na data de sua apresentação, sem inclusão de qualquer encargo financeiro ou previsão inflacionária e devem incluir todos os custos diretos, indiretos e despesas, necessárias a prestação dos serviços. O preço ofertado será irreajustável e constituirá a única e completa remuneração pelo cumprimento do objeto deste certame, não sendo aceitos pleitos de acréscimos nos preços, a qualquer título.

6.6.1. Quaisquer tributos, custos e despesas diretos ou indiretos serão considerados como inclusos nos preços, não sendo aceitos pleitos de acréscimo, a qualquer título.

6.7. A licitante declarada vencedora do certame deverá enviar a **PROPOSTA DE PREÇOS** conforme disposto no **Item 10.7**, de acordo com os formulários que seguem como **Anexo III deste Edital**, com todas as informações e declarações ali constantes, devendo ser redigida em língua portuguesa, com clareza, perfeitamente legível, sem emendas, rasuras, borrões, acréscimos ou entrelinhas, ser datada, rubricada em todas as folhas e assinada por seu representante legal ou procurador e respectivo cargo na licitante.

6.7.1. A proposta deverá ter validade de 60 (sessenta) dias corridos, contados a partir da data de sua apresentação.

7. ABERTURA DA SESSÃO E CLASSIFICAÇÃO INICIAL DAS PROPOSTAS DE PREÇOS

7.1. Na data e horário indicados no preâmbulo deste Edital terá início automático a sessão pública do pregão eletrônico.

7.2. A análise da conformidade das propostas visará ao atendimento das condições estabelecidas neste Edital e seus anexos e será feita exclusivamente na fase de julgamento em relação à proposta mais bem classificada.

7.3. Serão desclassificadas as propostas:

a) cujo objeto não atenda as especificações, prazos e condições fixados neste edital e seus anexos;

b) que por ação da licitante ofertante contenham elementos que permitam a sua identificação;

c) Estipule preços inexequíveis ou acima do máximo definido para a contratação, global e unitariamente.

7.4. A desclassificação se dará por decisão motivada e registrada no sistema.

7.5. Serão desconsideradas ofertas ou vantagens baseadas nas propostas dos demais licitantes.

7.6. Somente as licitantes cujas propostas sejam classificadas e ordenadas automaticamente pelo sistema participarão da fase de lances.

8. ETAPA DE LANCES

8.1. Iniciada a etapa competitiva, as licitantes poderão encaminhar lances **exclusivamente por meio do sistema eletrônico**, sendo o licitante imediatamente informado do seu recebimento, registro e valor.

8.2. As licitantes poderão oferecer lances sucessivos, observado o horário fixado e as regras para sua aceitação.

8.3. A Licitante somente poderá oferecer lance inferior ou percentual de desconto maior ao último por ela ofertado e registrado pelo sistema, observado o **intervalo mínimo de R$1,00 (um real)** em relação aos lances intermediários e em relação ao lance que cobrir a melhor oferta.

8.4. A licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 segundos após o registro do sistema, na hipótese de lance inconsistente ou inexequível.

8.5. As licitantes serão informadas, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

8.6. Na hipótese de o sistema eletrônico se desconectar no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.7. Caso a desconexão do sistema eletrônico persistir por tempo superior a dez minutos para o órgão ou a entidade promotora da licitação, a sessão pública será suspensa e reiniciada somente decorridas vinte e quatro horas após a comunicação do fato aos participantes, no sítio eletrônico utilizado para divulgação.

8.8. No caso de haver a participação de **MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE**, bem como de **COOPERATIVAS** que preencham as condições estabelecidas no artigo 1º, §2º, do Decreto nº 56.475/2015, no certame licitatório, os procedimentos obedecerão aos subitens a seguir:

8.8.1. Antes da classificação definitiva de preços, caso a melhor oferta não tenha sido apresentada por MICROEMPRESA, EMPRESA DE PEQUENO PORTE ou COOPERATIVA, o sistema utilizado verificará se ocorreu **EMPATE FICTO** previsto no § 2º do artigo 44 da Lei Complementar nº 123/2006 e Decreto Municipal nº 56.475/2015, ou seja, as propostas apresentadas por MICROEMPRESAS OU EMPRESAS DE PEQUENO PORTE que preenchas as condições estabelecidas no artigo 1º, §2º, do Decreto nº 56.475/2015, com valores até 5% (cinco por cento) acima do melhor preço ofertado.

8.8.2. Em caso positivo, a MICROEMPRESA, EMPRESA DE PEQUENO PORTE ou COOPERATIVA convocada poderá apresentar proposta de preço inferior àquela, à primeira classificada no prazo de 5 (cinco) minutos, sob pena de preclusão.

8.8.3. Caso a MICROEMPRESA (ME), EMPRESA DE PEQUENO PORTE (EPP) ou COOPERATIVA (COOP) convocada não exerça o benefício de ofertar preço inferior à primeira classificada ou não o faça no tempo aprazado, o sistema automaticamente convocará as ME/EPP/COOP remanescentes que, porventura, se enquadrem na hipótese do empate ficto, na ordem classificatória, para exercício do mesmo direito, sucessivamente, se for o caso.

8.8.4. Se houver equivalência entre os valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos apontados nos itens anteriores, será realizado sorteio para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.9. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

8.10. Em caso de eventual empate entre propostas ou lances, serão adotados os critérios previstos no art. 60 da Lei 14.133/21, de acordo com a ordem legalmente estabelecida.

8.11. Após a etapa de lances, se a melhor proposta estiver em desconformidade com o preço máximo estipulado para a contratação, o Pregoeiro poderá negociar melhores condições.

8.12. Quando o primeiro colocado, em que pese a negociação realizada, mantiver sua proposta acima do preço máximo definido, a negociação poderá ser realizada com os demais licitantes.

8.13. A negociação será realizada por meio do sistema, com acompanhamento dos demais licitantes e divulgação do resultado, bem como anexação aos autos do processo.

8.14. O licitante mais bem classificado deverá, **no prazo de 1 (uma) hora**, prorrogável a partir e solicitação fundamentada, enviar a **PROPOSTA DE PREÇOS**, adequada ao último lance ofertado após a negociação, além dos documentos de habilitação conforme item 11.7.

8.15. Encerrada a negociação, o pregoeiro iniciará a fase de aceitação e julgamento da proposta.

9. MODO DE DISPUTA ABERTO E FECHADO

9.1. Os licitantes apresentarão lances públicos e sucessivos, com lance final fechado.

9.2. No modo de disputa **ABERTO E FECHADO** a etapa de envio de lances terá duração de 15 (quinze) minutos.

9.3. Decorrido o prazo inicial, o sistema encaminhará aviso de fechamento iminente dos lances e, transcorrido o período de até 10 (dez) minutos, aleatoriamente determinado, a recepção de lances será automaticamente encerrada.

9.4. Em sequência, será aberta oportunidade para que o autor da oferta de valor mais baixo, bem como os das ofertas com valores de até 10% (dez por cento) superiores possam apresentar lance final e fechado em até 5 (cinco) minutos, podendo os licitantes, nestas condições, optarem por manter o último lance da etapa aberta ou ofertar melhor lance. O lance final será sigiloso até o encerramento deste prazo.

9.5. Na ausência de, no mínimo, três ofertas nas condições de que trata o item anterior, os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, poderão oferecer um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento do prazo.

9.6. Expirados os prazos, o sistema ordenará e divulgará os lances.

10. JULGAMENTO

10.1. Para julgamento e classificação das propostas será adotado o critério do **MENOR PREÇO TOTAL**, observados os requisitos, as especificações técnicas e os parâmetros definidos neste Edital e em seus anexos quanto ao objeto.

10.2. Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro realizará a verificação da conformidade da proposta classificada em primeiro lugar quanto à adequação ao objeto estipulado, à compatibilidade do preço ou maior desconto final em relação ao estimado para a contratação.

10.3. É recomendável, nesta fase, que sejam **consultados os cadastros previstos no item 11.8.8**, em nome da empresa licitante e também de seu sócio majoritário, de forma a verificar a existência de sanção que impeça a participação no certame e futura contratação, garantida a manifestação do licitante previamente a eventual desclassificação.

10.4. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum benefício direcionado às ME/EPP's, o Pregoeiro diligenciará para verificar o enquadramento.

10.5. Será desclassificada a proposta vencedora que não atender aos requisitos do **item 6.7**.

10.6. Erros no preenchimento da proposta não constituem motivo para desclassificação da proposta, desde que se limitem a erros ou falhas que não alteram a substância da proposta.

10.7. Após a negociação, o Pregoeiro fará o exame da aceitabilidade da oferta da primeira classificada, devendo esta anexar no sistema eletrônico, em prazo estabelecido pelo Pregoeiro, sob pela de desclassificação, a **PROPOSTA DE PREÇO** com o valor do preço final alcançado, e documentos de habilitação conforme item 11.7.

10.8. O Pregoeiro deverá verificar, como critério de aceitabilidade, a compatibilidade do menor preço, inclusive quanto aos preços unitários, alcançado com os parâmetros de preços de mercado, definidos pela Administração, coerentes com a execução do objeto licitado, aferido mediante a pesquisa de preços que instrui o processo administrativo pertinente a esta licitação.

10.9. Em caso de incompatibilidade de algum valor unitário com os parâmetros da Administração, estes poderão ser negociados com o licitante provisoriamente classificado em primeiro lugar, sem possibilidade de majoração do preço final alcançado na fase de lances.

10.10. Se o preço alcançado ensejar dúvidas quanto a sua exequibilidade, poderá o Pregoeiro determinar à licitante que demonstre a sua viabilidade, sob pena de desclassificação, por meio de documentação complementar que comprove a capacidade da licitante em fornecer o objeto licitado pelo preço ofertado e nas condições propostas no Edital.

10.11. Se a oferta não for aceitável ou se a licitante não atender à exigência estabelecida na cláusula supra, o Pregoeiro, desclassificará, motivadamente, a proposta e examinará as ofertas subsequentes, na ordem de classificação, até a apuração de uma proposta que atenda a todas as exigências, devendo, também, negociar diretamente com a proponente, para que seja obtido preço melhor.

10.12. Considerada aceitável a oferta de menor preço, passará o Pregoeiro ao julgamento da habilitação.

11. HABILITAÇÃO

11.1. Divulgado o julgamento das propostas de preços na forma prescrita neste Edital, passar-se-á à fase de habilitação.

11.2. Caso os dados e informações constantes do SICAF não atendam aos requisitos exigidos deste Edital, o Pregoeiro verificará a possibilidade de alcançar os documentos por meio eletrônico, juntando-os ao processo administrativo pertinente à licitação.

11.2.1. Sob pena de desclassificação, a licitante, cuja oferta foi aceita, deverá anexar no sistema eletrônico a **PROPOSTA DE PREÇOS** e a documentação exigida no subitem 11.7, no prazo estabelecido pelo Pregoeiro.

11.3. A documentação relativa a **Habilitação Jurídica** **sempre** deverá ser encaminhada pela licitante, para identificar os sócios/representantes que subscrevem a proposta e demais documentos por ela emitidos.

11.4. O Pregoeiro e sua Equipe de Apoio alcançarão dos documentos exigidos no subitem 11.7 deste Edital, por meio eletrônico, devendo a licitante encaminhar pelo sistema os demais documentos não emitidos via Internet.

11.4.1. Na impossibilidade de obtenção/emissão de documentos por meio eletrônico, o Pregoeiro solicitará sua apresentação pela licitante, juntamente com os demais documentos.

11.5. Tratando-se de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

11.5.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% para o consórcio em relação ao valor exigido para os licitantes individuais.

11.6. A Administração não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos hábeis de informações no momento da verificação de documentação ou dos meios para a transmissão de documentos a que se referem as cláusulas anteriores, ressalvada a indisponibilidade de seus próprios meios. Na hipótese de ocorrerem essas indisponibilidades, a licitante deverá encaminhar os documentos solicitados por outros meios, dentro do prazo estabelecido, sob pena de inabilitação, mediante decisão motivada.

11.6.1. Por meio de aviso lançado no sistema, via "CHAT", o Pregoeiro informará às demais licitantes a empresa habilitada por atendimento às condições estabelecidas neste Edital.

11.7. A habilitação se dará mediante o exame dos documentos a seguir relacionados, relativos a:

11.7.1. HABILITAÇÃO JURÍDICA:

a) Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

b) Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede; Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

c) Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

d) Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

e) Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

f) Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

g) Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

11.7.1.1. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.7.2. REGULARIDADE FISCAL E TRABALHISTA:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

b) Prova de inscrição no cadastro de contribuintes Estadual e/ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

d) Certidão de regularidade de débitos referentes a tributos estaduais relacionados com o objeto licitado, expedida por meio de unidade administrativa competente da sede ou domicílio da licitante;

d.1) No caso da licitante ter domicílio ou sede no Estado de São Paulo, a prova de regularidade para com a Fazenda Estadual se dará através da certidão de débitos tributários da Dívida Ativa do Estado de São Paulo, expedida nos termos da Resolução Conjunta SF/PGE nº 02, ou a que suceder.

e) Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

f) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

g) Certidão Negativa de Débitos Tributários Mobiliários, relativos ao Município de São Paulo, expedida pela Secretaria Municipal da Fazenda;

g.1) Caso a licitante não esteja localizada neste Município, deverá apresentar declaração firmada pelo seu representante legal/procurador, sob as penas da lei, do não cadastramento e de que nada deve à Fazenda do Município de São Paulo, relativamente aos tributos relacionados com a prestação licitada, conforme modelo do **Anexo V**.

11.7.2.1. Serão aceitas como prova de regularidade, certidões positivas com efeito de negativas.

11.7.2.2. Caso o fornecedor seja considerado isento dos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

11.7.2.3. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

11.7.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

a) Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples.

b) Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

11.7.4. QUALIFICAÇÃO TÉCNICA:

a) Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

a.1) Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

I) Serviços de segurança de tecnologia da informação para clientes que possuam pelo menos 1000 ativos de rede.

a.2) Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

a.3) Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

a.4) O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

11.7.5. OUTROS DOCUMENTOS:

a) Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo na condição de aprendiz, a partir de 14 anos, sob as penas da Lei, conforme o disposto no artigo. 7º, inciso XXXIII da Constituição Federal e inciso VI do art. 68 da Lei Federal nº 14.133/21;

b) Declaração de inexistência de fato superveniente impeditivo de sua habilitação inclusive condenação judicial na proibição de contratar com o Poder Público ou receber benefícios ou incentivos fiscais ou creditícios, transitada em julgada ou não desafiada por recurso com efeito suspensivo, por ato de improbidade administrativa;

c) Declaração de que a licitante não possui sanções vigentes previstas no inciso III do art. 156 da Lei Federal nº 14.133/21, no âmbito da Administração Pública Direta e indireta do Município de São Paulo e no inciso IV do mesmo artigo, no âmbito de quaisquer entes federativos;

d) Em se tratando de ME e EPP, declaração de observância e atendimento aos parágrafos §1º, §2º, §3º do art. 4º da Lei Federal nº 14.133/21;

e) Declaração que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na CF/88, leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, sob pena de desclassificação;

f) Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social conforme inciso IV do art. 63 da Lei 14.133/2021;

f.1) Será realizada consulta junto ao Ministério do Trabalho e Emprego (https://certidoes.sit.trabalho.gov.br/pcdreab), e no caso da certidão apresentar percentual inferior do previsto no art. 93 da Lei 8.213/91, a empresa será inabilitada.

g) Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

11.7.5.1. As declarações supra deverão ser elaboradas em papel timbrado e subscritas pelo representante legal da licitante, sendo recomendada a utilização do modelo constante no **ANEXO IV do presente Edital, facultando-se a elaboração de declarações individualizadas.**

11.8. A licitante para fins de habilitação deverá observar as disposições gerais que seguem:

11.8.1. Todos os documentos devem estar com seu prazo de validade em vigor. Se este prazo não constar de cláusula específica deste edital, do próprio documento ou de lei específica, será considerado o prazo de validade de 06 (seis) meses, a contar da data de sua expedição, salvo os atestados/certidões de qualificação técnica, para os quais não se exige validade.

11.8.2. Todos os documentos expedidos pela empresa deverão estar subscritos por seu representante legal ou procurador, com identificação clara do subscritor.

11.8.3. Os documentos emitidos via Internet serão conferidos pelo Pregoeiro ou sua equipe de apoio.

11.8.4. Se a licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.8.4.1. Caso a licitante pretenda que um de seus estabelecimentos, que não o participante desta licitação, execute o futuro contrato, deverá apresentar toda documentação de habilitação de ambos os estabelecimentos.

11.8.4.2. Atestados de capacidade técnica ou de responsabilidade técnica podem ser apresentados em nome e com o número do CNPJ (MF) da matriz ou da filial da empresa licitante.

11.8.5. Todo e qualquer documento apresentado em língua estrangeira deverá estar acompanhado da respectiva tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

11.8.6. Não serão aceitos documentos cujas datas e caracteres estejam ilegíveis ou rasurados de tal forma que não possam ser entendidos.

11.8.7. Os documentos exigidos para habilitação não poderão, em hipótese alguma, ser substituídos por protocolos, que apenas configurem o seu requerimento, não podendo, ainda, ser remetidos posteriormente ao prazo fixado.

11.8.8. O Pregoeiro e sua Equipe de Apoio verificarão eventual descumprimento das vedações de participação na licitação, mediante consulta ao:

a) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça – CNJ, no endereço eletrônico www.cnj.jus.br/improbidade_adm/consultar_requerido.php;

b) Cadastro Nacional das Empresas Inidôneas e Suspensas – CEIS, no endereço eletrônico https://www.portaltransparencia.gov.br/sancoes/ceis;

c) Portal de Sanções Administrativas, no endereço eletrônico https://www.bec.sp.gov.br/Sancoes_ui/aspx/sancoes.aspx;

d) Rol de Empresas Punidas, disponível no endereço eletrônico http://www.prefeitura.sp.gov.br/cidade/secretarias/gestao/suprimentos_e_servicos/empresas_punidas/index.php?p=9255;

e) Cadastro Nacional de Empresas Punidas (CNEP), disponível no endereço eletrônico https://www.portaltransparencia.gov.br/sancoes/cnep;

11.8.8.1. As consultas realizar-se-ão em nome da licitante e também de eventual matriz ou filial e de seus sócios majoritários.

11.9. Os documentos serão analisados pelo Pregoeiro e sua Equipe de Apoio quanto a sua conformidade com os solicitados e serão anexados ao processo administrativo pertinente a esta licitação.

11.9.1. Estando a documentação de habilitação da licitante vencedora em desacordo com as exigências do Edital, ela será inabilitada.

11.9.1.1. Havendo alguma restrição na comprovação da regularidade fiscal de microempresa ou empresa de pequeno porte assim qualificada, que preencha as condições estabelecidas no artigo 1º, §2º, do Decreto nº 56.475/2015, a sessão será suspensa, concedendo-se o prazo de 5 (cinco) dias úteis, prorrogável por igual período, para regularização, de forma a possibilitar, após tal prazo, sua retomada, nos termos do disposto no artigo 17 do Decreto nº 56.475/2015.

11.9.2. Sendo inabilitada a proponente cuja proposta tenha sido classificada em primeiro lugar, o Pregoeiro examinará a proposta ou lance subsequente, verificando sua aceitabilidade e procedendo à habilitação da licitante, na ordem de classificação, e assim sucessivamente até a apuração de uma proposta ou lance e proponente que atendam o Edital.

11.9.3. Os documentos relativos à regularidade fiscal somente serão exigidos em momento posterior ao julgamento das propostas e apenas do licitante mais bem classificado, salvo na hipótese de inversão de fases; caso em que os licitantes deverão encaminhar a proposta e, simultaneamente, os documentos de habilitação, por meio do sistema.

11.9.4. Após o envio dos documentos de habilitação, não será admitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência para complementação de informações em relação aos documentos já apresentados e desde que necessária para apurar fatos existentes à época da abertura do certame e atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

11.9.5. Estando a documentação de habilitação da licitante completa, correta, com observância de todos os dispositivos deste Edital e seus Anexos o Pregoeiro considerará a proponente habilitada e vencedora do certame.

12. FASE RECURSAL

12.1. Qualquer licitante poderá, durante o prazo concedido na sessão pública, não inferior a 10 minutos, de forma imediata após o término do julgamento das propostas e do ato de habilitação ou inabilitação, em campo próprio do sistema, manifestar sua intenção de recorrer, sob pena de preclusão, ficando a autoridade superior autorizada a adjudicar o objeto ao licitante declarado vencedor.

12.2. As razões do recurso deverão ser apresentadas em momento único, em campo próprio no sistema, no prazo de três dias úteis, contados a partir da data de intimação ou de lavratura da ata de habilitação ou inabilitação ou, na hipótese de adoção da inversão de fases, da ata de julgamento, a apresentação de documentos relativos às peças antes indicadas, se houver, será efetuada mediante protocolo, no endereço constante do preâmbulo deste Edital, das 08h00 às 17h00, observados os prazos estabelecidos no subitem 12.1.

12.3. Os demais licitantes ficarão intimados para, se desejarem, apresentar suas contrarrazões, no prazo de três dias úteis, contado da data de intimação pessoal ou de divulgação da interposição do recurso.

12.4. Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

12.5. O acolhimento do recurso importará na invalidação apenas dos atos que não possam ser aproveitados.

12.6. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão, a qual poderá reconsiderar a decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contados do recebimento dos autos.

12.7. O recurso e pedido de reconsideração terão efeito suspensivo até a decisão final pela autoridade competente.

13. ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior para adjudicar o objeto e homologar o procedimento, observado o disposto no art. 71 da Lei nº 14.133, de 2021.

14. PREÇO, REAJUSTE E DOTAÇÃO

14.1. O preço que vigorará no ajuste será o ofertado pela licitante a quem for o mesmo adjudicado.

14.2. Este preço inclui todos os custos diretos e indiretos, impostos, taxas, benefícios, encargos sociais, trabalhistas e fiscais que recaiam sobre o objeto, incluindo frete até o local de entrega designado pela Prefeitura, transporte, etc, e constituirá, a qualquer título, a única e completa remuneração pelo seu adequado e perfeito cumprimento, de modo que nenhuma outra remuneração será devida.

14.3. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data de assinatura do contrato.

14.3.1. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Preços ao Consumidor – IPC, apurado pela Fundação Instituto de Pesquisas Econômicas – FIPE, nos termos da Portaria SF n.º 389/17, bem como Decreto Municipal nº 57.580/17, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade

14.3.1.1. Eventuais diferenças entre o índice geral de inflação efetivo e aquele acordado na cláusula 14.3.1 não geram, por si só, direito ao reequilíbrio econômico financeiro do contrato.

14.3.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste

14.3.3. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

14.3.4. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s.
14.3.5. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

14.3.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

14.3.7. O reajuste será realizado por apostilamento.

14.3.8. Será aplicada compensação financeira, nos termos da Portaria SF nº 05, de 05 de janeiro de 2012, quando houver atraso no pagamento dos valores devidos, por culpa exclusiva da Contratante, observada a necessidade de se apurar a responsabilidade do servidor que deu causa ao atraso no pagamento, nos termos legais.

14.3.9. Fica ressalvada a possibilidade de alteração das condições contratuais em face da superveniência de normas federais e/ou municipais que as autorizem

14.4. Os recursos necessários para suporte do contrato, onerarão a dotação nº **17.20.04.126.3011.2.818.3.3.90.40.00.08.1.759.1383.1** do orçamento vigente.

15. CONDIÇÕES DO AJUSTE E GARANTIA PARA CONTRATAR

15.1. A contratação decorrente desta licitação será formalizada mediante termo de contrato, a ser firmado entre as partes, conforme minuta do Anexo I deste Edital.

15.1.1. Para a formalização do ajuste a empresa adjudicatária do objeto da licitação deverá apresentar os documentos já exigíveis por ocasião da habilitação, aqueles necessários à contratação, atualizados, caso solicitados.

15.1.2. Como condição à contratação, ainda, **deverá restar comprovado que a empresa a ser contratada não possui pendências junto ao Cadastro Informativo Municipal – CADIN MUNICIPAL**, por força da Lei Municipal nº 14.094/2005 e Decreto nº 47.096/2006, que disciplinam que a inclusão no CADIN impedirá a empresa de contratar com a Administração Municipal.

15.2. O prazo para assinatura do Contrato será de 05 (cinco) dias úteis, contados da data da publicação da convocação da adjudicatária no Diário Oficial da Cidade (D.O.C.), sob pena de decadência do direito à contratação, sem prejuízo das sanções descritas no Item 18 deste edital.

15.2.1. O prazo para formalização do ajuste, poderá ser prorrogado uma vez, por igual período, desde que solicitado por escrito, durante seu transcurso e ocorra motivo justificado e aceito pela Administração.

15.2.2. O Contrato deverá ser assinado por representante legal, diretor ou sócio da empresa, com apresentação, conforme o caso e, respectivamente, de procuração ou contrato social, acompanhados de cédula de identidade.

15.3. É facultado à Administração, quando o convocado não formalizar o ajuste no prazo e condições estabelecidos, inclusive na hipótese de impedimento da contratação, sem embargo da aplicação das penalidades cabíveis, retomar o procedimento, mediante agendamento de nova Sessão Pública, ou revogar a licitação.

15.3.1. Na hipótese de retomada do procedimento, as demais licitantes classificadas serão convocadas para participar da nova sessão pública do pregão, com vistas a celebração da contratação.

15.3.2. O aviso da nova sessão será publicado no Diário Oficial da Cidade e divulgação no endereço eletrônico https://www.gov.br/compras – UASG 925011 – SECRETARIA MUNICIPAL DA FAZENDA.

15.3.3. Na sessão o Pregoeiro convocará as licitantes classificadas remanescentes, na ordem de classificação, promovendo a averiguação das condições de aceitabilidade de preços e de habilitação, procedendo-se conforme especificações deste edital, até o encontro de uma proposta e licitante que atendam a todas as exigências estabelecidas, sendo a respectiva licitante declarada vencedora e a ela adjudicado o objeto da licitação.

15.4. A adjucataria:

a) não poderá subcontratar, ceder ou transferir o objeto do Contrato, no todo ou em parte, a terceiros, sob pena de rescisão;

15.5. Deverá ser prestada a **GARANTIA** conforme consta da minuta do termo de contrato, Anexo I deste Edital.

16. PRAZO PARA INÍCIO DOS SERVIÇOS E VIGÊNCIA CONTRATUAL

16.1. A Administração estabelecerá data certa para início da execução do serviço, conforme constar na Minuta de Contrato (Anexo I) ou, excepcionalmente, por meio de Ordem de Início dos Serviços.

16.1.1. O serviço deverá ser prestado de acordo com o ofertado na proposta, atendendo a todas as condições do Termo de Referência – Anexo II, correndo por conta da contratada todas as despesas decorrentes da execução do objeto contratual.

16.2. O prazo de vigência do contrato é de 36 (trinta e seis) meses, contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133/2021, e do artigo 116 do Decreto Municipal n.º 62.100, de 2022, desde que haja concordância das partes, o contratado haja cumprido satisfatoriamente suas obrigações, bem como a pesquisa prévia revele que os preços são compatíveis com os de mercado, nos termos previstos na minuta de contrato - Anexo I deste Edital.

16.3. Caso a Contratada não tenha interesse na prorrogação do ajuste deverá comunicar este fato por escrito à Contratante, com antecedência mínima de 90 (noventa) dias da data de término do prazo contratual, sob pena de incidência de penalidade contratual.

16.4. Na ausência de expressa oposição, e observadas as exigências contidas nos incisos I e II do artigo 116 do Decreto Municipal n.º 62.100, de 2022, o ajuste poderá, a critério da Administração Pública, ser prorrogado, mediante despacho da autoridade competente.

16.4.1. A não prorrogação do prazo de vigência contratual, por conveniência da Administração, não gerará à Contratada o direito a qualquer espécie de indenização.

16.5. Não obstante o prazo estipulado no subitem 16.2, a vigência contratual nos exercícios subsequentes ao da assinatura do contrato estará sujeita à condição resolutiva, consubstanciada na existência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício, para atender as respectivas despesas.

16.6. A DATA DE INÍCIO DA PRESTAÇÃO DOS SERVIÇOS será certificada pela unidade responsável pelo acompanhamento da execução contratual.

17. CONDIÇÕES DE RECEBIMENTO E PAGAMENTO

17.1. As cláusulas relativas ao recebimento dos serviços e pagamento são as constantes da minuta de termo de contrato, Anexo I deste Edital.

17.2. Observar-se-á o quanto disposto na Lei 14.133/21 e Decreto nº 62.100/22, a respeito da nomeação de fiscais e acompanhamento da execução, até o seu término.

18. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

18.1. São aplicáveis as sanções e procedimentos previstos no Título IV, Capítulo I da Lei Federal nº 14.133/21 e Capítulo VI, Seção XI do Decreto Municipal nº 62.100/22.

18.1.1. As penalidades só deixarão de ser aplicadas nas seguintes hipóteses:

a) comprovação, anexada aos autos, da ocorrência de força maior impeditiva do cumprimento da obrigação; e/ou,

b) manifestação da unidade requisitante, informando que o ocorrido derivou de fatos imputáveis exclusivamente à Administração.

18.2. Ocorrendo recusa da adjudicatária em retirar/receber a nota de empenho, dentro do prazo estabelecido neste Edital, sem justificativa aceita pela Administração, garantido o direito prévio de citação e da ampla defesa, serão aplicadas:

a) Multa no valor de 20% (vinte por cento) do valor do ajuste se firmado fosse;

b) Pena de impedimento de licitar e contratar pelo prazo de até 3 (três) anos com a Administração Pública, a critério da Prefeitura;

18.2.1. Incidirá nas mesmas penas previstas neste subitem a empresa que estiver impedida de firmar o ajuste pela não apresentação dos documentos necessários para tanto.

18.3. À licitante que ensejar o retardamento da execução do certame, inclusive em razão de comportamento inadequado de seus representantes, deixar de entregar ou apresentar documentação falsa exigida neste edital, não mantiver a proposta/lance, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, se microempresa ou pequena empresa não regularizar a documentação fiscal no prazo concedido para este fim, garantido o direito prévio de citação e da ampla defesa, serão aplicadas as penalidades referidas nas alíneas "a" e "b" do subitem 18.2 ou declaração de inidoneidade para licitar ou contratar, a depender da natureza e gravidade da infração cometida e peculiaridades do caso em concreto.

18.4. As penalidades poderão ainda ser aplicadas em outras hipóteses, nos termos da Lei, garantido o direito prévio de citação e da ampla defesa, sendo que com relação a execução do contrato, as multas serão aplicadas conforme descrito no Anexo I – Minuta Termo de Contrato. As sanções são independentes e a aplicação de uma não exclui a das outras, quando cabíveis.

18.5. Das decisões de aplicação de penalidade, caberá recurso nos termos do artigo 157 da Lei Federal nº 14.133/21, observados os prazos nele fixados.

18.5.1. Caso a Contratante releve justificadamente a aplicação da multa ou de qualquer outra penalidade, essa tolerância não poderá ser considerada como modificadora de qualquer condição contratual, permanecendo em pleno vigor todas as condições deste Edital.

18.6. Os procedimentos de aplicação das penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar e contratar serão conduzidos por comissão, nos termos do artigo 158, "caput" e § 1º, da Lei Federal nº 14.133/21.

18.7. São aplicáveis à presente licitação e ao ajuste dela decorrente no que cabível for, inclusive, as sanções penais estabelecidas na Lei Federal nº 14.133/21.

19. DISPOSIÇÕES GERAIS

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

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

19.3. As licitantes assumem todos os custos de preparação e apresentação de suas propostas e a PMSP não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

19.4. As licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do certame.

19.4.1. A falsidade de qualquer declaração prestada poderá caracterizar o crime de que trata o art. 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e das sanções administrativas previstas na legislação pertinente, mediante o devido processo legal, e implicará, também, a inabilitação da licitante se o fato vier a ser constatado durante o trâmite da licitação.

19.5. A licitante vencedora deverá comunicar à Administração toda e qualquer alteração nos dados cadastrais, para atualização, devendo manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

19.6. O ajuste, suas alterações e rescisão obedecerão à Lei Federal nº 14.133/21, demais normas complementares e disposições deste Edital, aplicáveis à execução dos contratos e especialmente os casos omissos.

19.7. A revogação ou anulação da licitação observará os procedimentos e normas previstas no art. 71 da Lei Federal nº 14.133/21.

19.8. O Pregoeiro poderá promover diligências destinada à complementação de informações sobre documentos já apresentados, desde que se tratem de fatos existentes à época da abertura do certame e atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas, nos termos do art. 64 da Lei Federal nº 14.133/21.

19.9. Os casos omissos e as dúvidas surgidas serão resolvidos pelo Pregoeiro ouvidas, se for o caso, as Unidades competentes.

19.10. Integrarão o ajuste a ser firmado, para todos os fins, a proposta da Contratada, a Ata da licitação e o Edital da Licitação, com seus anexos, que o precedeu, independentemente de transcrição.

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

19.12. A Contratada não poderá subcontratar, ceder ou transferir o objeto do contrato, no todo ou em parte, a terceiros, sob pena de rescisão.

19.13. Fica ressalvada a possibilidade de alteração das condições contratuais em face da superveniência de normas federais e municipais disciplinando a matéria.

19.14. Na contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento, observado o art. 183 da Lei Federal 14.133/21.

19.15. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário estabelecido, desde que não haja comunicação em contrário do Pregoeiro.

19.16. Os atos relativos à licitação efetuados por meio do sistema serão formalizados e registrados em processo administrativo pertinente ao certame.

19.17. O resultado deste Pregão e os demais atos pertinentes a esta licitação, sujeitos a publicação, serão divulgados no Diário Oficial da Cidade (https://diariooficial.prefeitura.sp.gov.br/) e no sítio eletrônico https://www.gov.br/compras/pt-br, bem como no Portal Nacional de Contratações Públicas – PNCP.

19.18. O Pregoeiro e a Equipe de Apoio que atuarão neste pregão eletrônico foram designados nos autos do processo administrativo a ele pertinente e indicados no sistema.

19.19. Qualquer divergência entre as especificações contidas no Anexo II deste Edital e as constantes no catálogo de serviços afeto ao sistema COMPRASNET, **PREVALECERÃO PARA TODOS OS EFEITOS AS DO ANEXO II.**

19.20. O Edital e seus anexos estão disponíveis no Portal Nacional de Contratações Públicas (PNCP) e endereços eletrônicos https://www.gov.br/compras/pt-br e https://diariooficial.prefeitura.sp.gov.br/.

19.21. As dúvidas interpretativas e eventuais omissões serão realizadas com plena observância ao disposto nas normas previstas na Lei Federal 14.133/21 e no Decreto Municipal nº 62.100/22.

19.22. Fica desde logo eleito o Foro da Comarca da Capital – Vara da Fazenda Pública - para dirimir quaisquer controvérsias decorrentes do presente certame ou de ajuste dele decorrente.

FABIANA APARECIDA OLIVEIRA PEREIRA:[redacted]

Assinado de forma digital por FABIANA APARECIDA OLIVEIRA PEREIRA:[redacted]
Dados: 2023.11.14 14:59:00 -03'00'

FABIANA A. O. PEREIRA – Pregoeira

Secretaria Municipal da Fazenda – UASG 925011

CIDADE DE SÃO PAULO
FAZENDA

ANEXO I – MINUTA DE TERMO DE CONTRATO

TERMO DE CONTRATO SF Nº

PROCESSO: 6017.2023/0033846-3

PREGÃO ELETRONICO Nº 17/2023

OBJETO: Contratação de serviços de Segurança da Informação (SOC – Security Operations Center), pelo período de 36 meses, conforme condições e exigências estabelecidas no Termo de Referência – Anexo II.

CONTRATANTE: Prefeitura do Município de São Paulo – Secretaria Municipal da Fazenda

CONTRATADA:

VALOR DO CONTRATO:

DOTAÇÃO ORÇAMENTÁRIA: 17.20.04.126.3011.2.818.3.3.90.40.00.08.1.759.1383.1

O Município de São Paulo, por sua **Secretaria Municipal da Fazenda**, inscrita no CNPJ sob o nº 46.392.130/0001-18, com sede na Rua Líbero Badaró, nº 190 – Edifício Othon – 22º andar, Centro, São Paulo/SP, CEP 01008-000, neste ato representada pelo Chefe de Gabinete, Senhor **EVANDRO LUIS ALPOIM FREIRE**, adiante denominada simplesmente **CONTRATANTE**, e a empresa ....., inscrita no CNPJ sob o nº ....., com sede na ....., neste ato representada por ..... (nome e função no contratado e CPF), conforme atos constitutivos da empresa **OU** procuração apresentada nos autos, adiante denominada simplesmente **CONTRATADA,** nos termos da autorização contida no Processo acima citado e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislações aplicáveis, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico SF nº 17/2023, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA - DO OBJETO DO CONTRATO

1.1. O objeto do presente instrumento é a contratação de serviços de Segurança da Informação (SOC – Security Operations Center), pelo período de 36 meses.

1.2. Vinculam esta contratação, independentemente de transcrição:

a) O Termo de Referência;
b) O Edital da Licitação;
c) A Proposta da CONTRATADA;
d) Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – DO LOCAL DE PRESTAÇÃO DOS SERVIÇOS

2.1. O datacenter principal da CONTRATANTE está localizado no Edifício Othon, na Rua Líbero Badaró, nº 190, Primeiro Subsolo - Centro, São Paulo - SP, doravante denominado datacenter. A CONTRATANTE poderá criar outros datacenters, extensões, alterar a localização ou excluir os mesmos.

2.1.1. Em caso de alteração da localização, criação de novos datacenters, criação de extensões ou exclusão destes, a CONTRATANTE deverá comunicará a CONTRATADA, sobre o início das operações na nova localidade com, no mínimo, 60 dias de antecedência.

2.2. São extensões do datacenter principal as unidades:

2.2.1. Controle Direto:

a) Gabinete - Vd. Do Chá, 15 - Ed. Matarazzo – Centro;

b) Nuvem.

2.2.2. Controle Indireto:

a) PRODAM Barra Funda: Av. Francisco Matarazzo, 1.500 - Ed. Los Angeles Água Branca;

b) PRODAM Pedro de Toledo, PRODAM - R Pedro de Toledo 983 - Vila Clementino.

2.3. O núcleo de operações e controle (NOC) da CONTRATANTE está localizado no Edifício Othon, na Rua Líbero Badaró, nº 190, Centro, São Paulo - SP.

2.4. O SOC – Security Operations Center, objeto principal do presente Termo de Referência, compreende o serviço contratado, o corpo profissional da CONTRATADA, os profissionais da CONTRATANTE envolvidos direta ou indiretamente com o objeto deste Termo de Referência, em regime de trabalho/operações presencial ou remoto.

2.5. As informações da CONTRATANTE deverão ser armazenadas unicamente nos locais definidos pela CONTRATANTE.

2.5.1. São dependências da CONTRATANTE:

a) Edifício Matarazzo, localizado no Viaduto do Chá, número 15, Anhangabaú, São Paulo - SP;

b) Edifício Othon, localizado na Rua Líbero Badaró, nº 190, Centro, São Paulo – SP.

CLÁUSULA TERCEIRA – VIGÊNCIA E PRORROGAÇÃO

3.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133, de 2021.

3.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a CONTRATADA, atentando, ainda, para o cumprimento dos 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 e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

d) Haja manifestação expressa da CONTRATADA informando o interesse na prorrogação;

e) Seja comprovado que a CONTRATADA mantém as condições iniciais de habilitação.

3.3. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

3.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

3.5. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

3.6. O contrato não poderá ser prorrogado quando a CONTRATADA tiver sido penalizada nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

CLÁUSULA QUARTA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

4.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4.2. Não será admitida a subcontratação do objeto contratual.

4.3. Os prazos das etapas dos serviços constam no item 8 do Termo de Referência – Anexo II.

CLÁUSULA QUINTA – DA GARANTIA CONTRATUAL

5.1. Será exigida a garantia da contratação de que tratam o art. 96 e seguinte da Lei nº 14.133/21, no percentual de 5% (cinco por cento) do valor contratual, conforme regras previstas no contrato.

5.2. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 10 (dias) dias após a assinatura do contrato.

5.3. Em caso opção pelo seguro-garantia, a parte adjudicatária terá prazo de 30 dias, contado da data de homologação da licitação, para sua apresentação, que deve ocorrer antes da assinatura do contrato.

CLÁUSULA SEXTA – DO PREÇO E DOTAÇÃO ORÇAMENTÁRIA

6.1. O valor total estimado para o período de 36 (trinta e seis) meses é de R$ _____ (_____).

6.2. O valor total mensal estimado da presente contratação é de R$ _____(_____).

ITEM	OBJETO	TIPO	MEDIÇÃO	QTDE MENSAL	VALOR UNITÁRIO	VALOR MENSAL	VALOR PARA 36 MESES
1	Serviço de gestão de vulnerabilidades	Aplicações Web	URL	154	R$...	R$...	R$...
		Ativos de Rede	Ips/Dispositivos	2.208	R$...	R$...	R$...
		Containers	Imagem de Container	130	R$...	R$...	R$...
2	Serviço de monitoramento de ataques cibernéticos	Correlacionamento de pacotes	EPS	4.000	R$...	R$...	R$...
		Detecção e resposta em Endpoint	Dispositivo	2.059	R$...	R$...	R$...
3	Serviço de respostas aos incidentes de segurança e de privacidade	Resposta Incidentes	UNIDADE	1	R$...	R$...	R$...
4	Serviço de inteligência aplicado à segurança	Monitoramento	UNIDADE	1	R$...	R$...	R$...
5	Serviços de Teste de Invasão	Reserva de Horas	Hora Homem	50	R$...	R$...	R$...
6	Serviços técnicos especializados	Reserva de Horas	Hora Homem	50	R$...	R$...	R$...

6.3. Todos os custos e despesas necessários à correta execução do ajuste estão inclusos no preço, inclusive os referentes às despesas trabalhistas, previdenciárias, impostos, taxas, emolumentos, em conformidade com o estatuído no Edital e seus Anexos, constituindo a única remuneração devida pela CONTRATANTE à CONTRATADA.

6.4. Para fazer frente às despesas do Contrato, foi emitida a Nota de Empenho nº ....., no valor de R$ .....(.....), onerando a dotação orçamentária nº **17.20.04.126.3011.2.818.3.3.90.40.00.08.1.759.1383.1** do orçamento vigente, respeitado o princípio da anualidade orçamentária, devendo as despesas do exercício subsequente onerar as dotações do orçamento próprio.

CLÁUSULA SÉTIMA – DO REAJUSTE

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data de assinatura do contrato.

7.2. Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, nos termos da Portaria SF nº 389 de 18 dezembro de 2017 pelo equivalente ao Índice de Preços ao Consumidor – IPC, apurado pela Fundação Instituto de Pesquisas Econômicas – FIPE, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA - PAGAMENTO

8.1. O faturamento decorre do escopo e tipo de serviço prestado, com respectivos quantitativos e valores, dentro do período mensal conforme item 6 do Termo de Referência – Anexo II.

8.2. O prazo de pagamento será de 30 (trinta) dias, contados da data da entrega da Nota Fiscal ou Nota Fiscal Fatura, nos moldes da Portaria SF 170/2020 e 187/2020.

8.2.1. Serão aceitas como prova de regularidade, certidões positivas com efeito de negativas e certidões positivas que noticiem em seu corpo que os débitos estão judicialmente garantidos ou com sua exigibilidade suspensa.

8.2.2. A não apresentação de certidões negativas de débito, ou na forma prevista no subitem 8.2.1 não impede o pagamento, porém será objeto de aplicação de penalidade ou rescisão contratual, conforme o caso.

8.2.3 Caso venha ocorrer a necessidade de providências complementares por parte da CONTRATADA, a fluência do prazo será interrompida, reiniciando-se a sua contagem a partir da data em que estas forem cumpridas.

8.2.4. Caso venha a ocorrer atraso no pagamento dos valores devidos, por culpa exclusiva da Administração, a CONTRATADA terá direito à aplicação de compensação financeira, nos termos da Portaria SF nº 05, de 05/01/2012.

8.2.5. Para fins de cálculo da compensação financeira de que trata o item 8.2.4, o valor do principal devido será reajustado utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança para fins de compensação da mora (TR + 0,5% "pro-rata tempore"), observando-se, para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

8.2.6. O pagamento da compensação financeira dependerá de requerimento a ser formalizado pela CONTRATADA.

8.3. Antes do pagamento a CONTRATANTE efetuará consulta ao Cadastro Informativo Municipal – CADIN MUNICIPAL, por força da Lei Municipal nº 14.094/2005 e Decreto nº 47.096/2006, do qual não poderá constar qualquer pendência.

8.4. Os pagamentos serão efetuados em conformidade com a execução dos serviços, mediante apresentação da(s) respectiva(s) nota(s) fiscal(is) ou nota(s) fiscal(is)/fatura, bem como de cópia reprográfica da nota de empenho, acompanhada, quando for o caso, do recolhimento do ISSQN – Imposto Sobre Serviços de Qualquer Natureza do mês de competência, descontados os eventuais débitos da CONTRATADA, inclusive os decorrentes de multas.

8.5. Na hipótese de existir nota de retificação e/ou nota suplementar de empenho, cópia(s) da(s) mesma(s) deverá(ão) acompanhar os demais documentos.

8.6. A CONTRATADA deverá apresentar, a cada pedido de pagamento, os documentos elencados na Portaria SF 170/2020.

8.7. Por ocasião de cada pagamento, serão feitas as retenções eventualmente devidas em função da legislação tributária.

8.8. O pagamento será efetuado por crédito em conta corrente, no BANCO DO BRASIL S/A, conforme estabelecido no Decreto nº 51.197/2010, publicado no DOC do dia 22 de janeiro de 2010.

8.9. Fica ressalvada qualquer alteração por parte da Secretaria Municipal da Fazenda, quanto às normas referentes ao pagamento de fornecedores.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E CONTRATADA

9.1. São obrigações da CONTRATANTE:

9.1.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com o contrato e seus anexos;

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

9.1.3. Notificar a CONTRATADA, 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, às suas expensas;

9.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela CONTRATADA;

9.1.5. Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

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

9.1.7. Aplicar à CONTRATADA as sanções previstas na lei e neste Contrato;

9.1.8. 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

9.1.9. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

9.1.10. A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

9.2. A CONTRATADA deve cumprir todas as obrigações constantes deste **CONTRATO, DO TERMO DE REFERÊNCIA E DEMAIS ANEXOS DO EDITAL**, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2.1. A CONTRATADA deverá designar formalmente PREPOSTO antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado de acordo com o item 6.4 do Termo de Referência.

9.2.2. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente da CONTRATANTE ou de agente público que tenha desempenhado função na licitação ou que atue na fiscalização ou gestão do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.2.3. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a CONTRATADA deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

1) prova de regularidade relativa à Seguridade Social;

2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede da CONTRATADA;

4) Certidão de Regularidade do FGTS – CRF; e

5) Certidão Negativa de Débitos Trabalhistas – CNDT.

9.2.4. Prestar todo esclarecimento ou informação solicitada pela CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do serviço.

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

9.2.6. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.2.7. Cumprir, durante todo o período de execução do contrato, a 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 na legislação (art. 116 da Lei 14.133/2021);

9.2.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.2.9. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

9.2.10. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da CONTRATANTE.

CLÁUSULA DÉCIMA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

10.1. São aplicáveis as sanções e procedimentos previstos no Título IV, Capítulo I da Lei Federal nº 14.133/21 e Seção XI do Decreto Municipal nº 62.100/22.

10.2. As penalidades só deixarão de ser aplicadas nas seguintes hipóteses:

a) comprovação, anexada aos autos, da ocorrência de força maior impeditiva do cumprimento da obrigação; e/ou,

b) manifestação da unidade requisitante, informando que o ocorrido derivou de fatos imputáveis exclusivamente à Administração.

10.3. Ocorrendo recusa da adjudicatária em retirar/receber a nota de empenho, dentro do prazo estabelecido para contratação, sem justificativa aceita pela Administração, garantido o direito prévio de citação e da ampla defesa, serão aplicadas:

a) Multa no valor de 20% (vinte por cento) do valor do ajuste se firmado fosse;

b) Pena de impedimento de licitar e contratar pelo prazo de até 3 (três) anos com a Administração Pública, a critério da Prefeitura

10.4. Incidirá nas mesmas penas previstas neste subitem a empresa que estiver impedida de firmar o ajuste pela não apresentação dos documentos necessários para tanto.

10.5. As penalidades poderão ainda ser aplicadas em outras hipóteses, nos termos da Lei, garantido o direito prévio de citação e da ampla defesa.

10.6. Pela inexecução total ou parcial do objeto desta contratação, a CONTRATANTE pode aplicar à CONTRATADA as seguintes sanções:

a) Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado

b) Multa de 0,5% (cinco décimos por cento), por dia sobre o valor total do ajuste, em caso de atraso no início da execução dos serviços, limitada a incidência a 10 (dez) dias. Após 10 (dez) dias de atraso será considerada inexecução parcial do contrato.

c) Multa de 1 % (um por cento), por dia sobre o valor total do ajuste, em caso de atraso no início da execução dos serviços, limitada a incidência do 11º (décimo primeiro) ao 20º (vigésimo) dia. Após o vigésimo dia será considerada inexecução total do ajuste.

d) Multa de 2% (dois por cento), sobre o valor total do ajuste, por não manter as mesmas condições da contratação quanto a regularidade fiscal e trabalhista, e na reincidência será aplicado o dobro;

e) Multa de 1% (um por cento), por dia de atraso, sobre o valor total do ajuste, por deixar de apresentar garantia contratual nos termos estipulados na contratação (seja inicial, reforço ou por ocasião de prorrogação), observado o máximo de 20% (vinte por cento). O atraso superior a 20 (vinte) dias autorizará a CONTRATANTE a promover a rescisão do contrato;

f) Multa de 3% (três por cento), sobre o valor mensal do ajuste, por descumprimento de qualquer obrigação da CONTRATADA para a qual não haja penalidade específica, por ocorrência e, na reincidência, será aplicado o dobro.

a) A cada reincidência, sobre o mesmo tipo de ocorrência, adiciona-se 1% aos 3% descritos acima. Até o limite de 10%.

b) Se a ocorrência acontecer após 6 meses da última, do mesmo tipo, será considerada nova incidência em detrimento de reincidência.

g) Multa de 10% (dez por cento), sobre o valor total do ajuste, por inexecução parcial do contrato.

h) Multa de 20% (vinte por cento), sobre o valor total do ajuste, no caso de rescisão do acordo, por culpa da CONTRATADA, inclusive por inexecução total do contrato, devida e previamente demonstrada a falta cometida à CONTRATADA;

i) Multa de 30% (trinta por cento), sobre o valor total do contrato, por deixar de comunicar à Secretaria a ocorrência de incidente de segurança; deixar de cumprir determinação da Secretaria para corrigir deficiências nos processos de tratamento; realizar cumprir determinação da Secretaria para o exercício de direito de titular de dados.

j) Multas específicas:

Para os casos de não atendimento, por parte da CONTRATADA, das etapas, marcos e prazos estipulados nos **itens 8.1, 8.2, 8.4, 8.5, 8.6 e 8.7** da **Especificação detalhada do objeto (1.1.1)**, de acordo com a tabela abaixo:

ITEM	DESCRIÇÃO	MULTA
8.1	Não atendimento aos prazos da etapa Iniciação	R$ 5.000,00
8.2	Não apresentação da proposta de solução	R$ 30.000,00 mais R$ 1.000 para cada dia de atraso
8.4	Não conclusão dos ambientes necessários para os serviços rotineiros	R$ 30.000,00 mais R$ 1.000 para cada dia de atraso
8.5	Não cumprimento dos prazos acerca dos entregáveis (relatórios e congêneres)	R$ 500,00 por dia de atraso
8.5	Não cumprimento da implementação das regras, parametrizações, configurações de ferramentas e congêneres	R$ 1.000,00 por dia de atraso
8.6	Não cumprimento do disposto em OS específica	Ver item **Multas sobre atividades projetizadas** abaixo (L)
8.7	Não cumprimento do item 8.7 no prazo estipulado	R$ 10.000,00 por dia de atraso
8.7	Não cumprimento do item 8.7	R$ 500.000,00

Dado que a documentação prevista no item 8.7 deve ser produzida ao longo da execução contratual, a CONTRATADA deverá apresentar a 180 dias da conclusão do contrato, proposta de documentação a ser entregue ao final do mesmo.

k) Multas aplicadas sobre o faturamento mensal das atividades rotineiras, nos seguintes percentuais:
a) 0,2% (dois décimos por cento) por dia de atraso, pela não substituição de profissional em até 30 dias corridos, quando requisitado pela CONTRATANTE.
b) 0,2% (dois décimos por cento), por dia, por linha de serviço, por profissional que não atenda às exigências do **Item 11 - Perfil Profissional** da **Especificação detalhada do objeto (1.1.1).**
c) 0,2% (dois décimos por cento), por dia de atraso, pelo não cumprimento do prazo de 15 (quinze) dias para iniciar a prestação dos serviços descritos em ordem de serviço, a partir de sua emissão.

l) Multas sobre atividades projetizadas:
Para os casos de não atendimento dos prazos, de acordo com a tabela abaixo:

ATIVIDADE	TEMPO DE ATENDIMENTO	MULTA APLICÁVEL
Confecção da Estimativa Prévia de Atividade Projetizada	Até 10 (dez) dias úteis após o envio da requisição.	R$250 por dia útil de atraso
Entrega final das atividades definidas na Atividade Projetizada	De acordo com o prazo acordado durante a emissão da OS (em dias úteis)	5% sobre o valor da OS acrescido de 0,5% por cada dia útil de atraso, até o valor total da OS

m) Glosas: para as atividades em suporte continuado (Item 8.5 da Especificação detalhada do objeto – 1.1.1) aplicam-se as glosas conforme abaixo:

Incidentes/ Requisição	Descrição	Tempo para resolução	Glosa aplicável
Severidade 1	Serviço indisponível para grande número de usuários e/ou com alta degradação de performance. Serviço indisponível para o público externo (contribuintes, cidadãos, etc.).	1 hora	2% + (0,8% para cada item - incidente ou resolução - fora da SLA e por dia de atraso na resolução)
Severidade 2	Serviço degradado, com risco iminente de indisponibilidade ou indisponível. Incidentes relacionados a usuários de alta prioridade (limitado a 3% dos usuários).	4 horas	2% + (0,3% para cada item - incidente ou requisição - fora da SLA e por dia de atraso na resolução)
Severidade 3	Serviço apresentando problemas sem indisponibilidade ou degradação de performance para os usuários, eventos de alertas proativos sem impacto de negócios.	6 horas	2% + (0,1% para cada item - incidente ou requisição - fora da SLA e por dia de atraso na resolução)
Rotineiro	Operações das ferramentas em geral tais como configuração de regras, parametrização de ferramentais, criação e/ou configurações de usuários	12 horas	2% + (0,05% para cada requisição fora da SLA e por dia de atraso)

10.7. As sanções são independentes e a aplicação de uma não exclui a das outras, quando cabíveis.

10.7.1. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

10.8. Caso a CONTRATANTE releve justificadamente a aplicação da multa ou de qualquer outra penalidade, essa tolerância não poderá ser considerada como modificadora de qualquer condição contratual, permanecendo em pleno vigor todas as condições da contratação.

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

10.10. Os procedimentos de aplicação das penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar e contratar serão conduzidos por comissão, nos termos do artigo 158, "caput" e § 1º, da Lei Federal nº 14.133, de 2021.

10.11. São aplicáveis à presente contratação e ao ajuste dela decorrente no que cabível for, inclusive, as sanções penais estabelecidas na Lei Federal nº 14.133/21.

10.12. 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).

10.13. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela CONTRATANTE à CONTRATADA, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

10.14. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

10.15. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser complementada no prazo de até 10 (dez) dias úteis, contado da solicitação da CONTRATANTE.

CLÁUSULA DÉCIMA PRIMEIRA – DA EXTINÇÃO CONTRATUAL

11.1. O contrato se extingue quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

11.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

11.3. Quando a não conclusão do contrato referida no item anterior decorrer de culpa da CONTRATADA:

a) ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

b) poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

11.4. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

11.5. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

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

11.7. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

11.8. O termo de rescisão, sempre que possível, será precedido:

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

11.8.2. Relação dos pagamentos já efetuados e ainda devidos;

11.8.3. Indenizações e multas.

11.9. A extinção do contrato não configura óbice para o reconhecimento do 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).

CLÁUSULA DÉCIMA SEGUNDA – DOS CASOS OMISSOS

12.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.3. 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.

CLÁUSULA DÉCIMA QUARTA - DO SIGILO DAS INFORMAÇÕES E DO TRATAMENTO DE DADOS

14.1. As informações que a CONTRATANTE fornecer, a seu exclusivo critério, para fins de execução do objeto contratual, serão mantidas em sigilo pela CONTRATADA e seus prepostos, comprometendo a CONTRATADA a:

a) Usar as informações para o único propósito de executar os serviços contratados;

b) Revelar as informações apenas para os membros de sua organização, necessários à condução do serviço contratado e requerer a eles que também mantenham o caráter confidencial dessas informações;

c) Obrigar-se a tratar como "segredos comerciais e confidenciais", e não fazer uso comercial de quaisquer informações e dados fiscais e tributários relativos aos serviços ora contratados, utilizando-os apenas para as finalidades previstas, não podendo revelá-los ou facilitar a sua revelação a terceiros, assim como não manter cópias ou arquivos após o término do serviço (dados protegidos pelo sigilo fiscal, conforme art. 198 da Lei Federal n.º 5.172, de 25 de outubro de 1966 – Código Tributário Nacional).

14.2. As obrigações de confidencialidade previstas no item 14.1 estendem-se aos funcionários, servidores, prestadores de serviços, prepostos e/ou representantes da CONTRATADA.

14.3. A obrigação de confidencialidade permanecerá após o término da vigência deste Contrato e sua violação

ensejará a aplicação à parte infratora da multa contratual prevista na **Cláusula Décima do item 10.6 – "i" deste instrumento**, sem prejuízo da responsabilidade civil e criminal.

14.4. Quaisquer tratamentos de dados pessoais realizados no bojo do presente CONTRATO, ou em razão dele, deverão observar as disposições da Lei nº 13.709, de 14 de agosto de 2018, e de normas complementares expedidas pela Autoridade Nacional de Proteção de Dados e pela CONTRATANTE.

14.5. Havendo necessidade de compartilhamento de dados pessoais no âmbito deste CONTRATO, serão transferidos apenas os dados estritamente necessários para a perfeita execução do objeto contratual, os quais deverão ser utilizadas apenas para tal fim.

14.5.1. O compartilhamento de dados, quando necessário, dar-se-á sempre em caráter sigiloso, sendo vedado à CONTRATADA transferir ou de qualquer forma disponibilizar as informações e os dados recebidos da CONTRATANTE a terceiros sem expressa autorização da CONTRATANTE.

14.5.2. No caso de transferência de dados a terceiros, previamente autorizada pela CONTRATANTE, a CONTRATADA deverá submeter o terceiro às mesmas exigências estipuladas neste instrumento no que se refere à segurança e privacidade de dados.

14.6. A CONTRATADA deverá eliminar quaisquer dados pessoais recebidos em decorrência deste CONTRATO sempre que determinado pela CONTRATANTE e, com expressa anuência da CONTRATANTE, nas seguintes hipóteses:

a) os dados se tornarem desnecessários;

b) término de procedimento de tratamento específico para o qual os dados se faziam necessários;

c) fim da vigência contratual.

14.7. A CONTRATADA deverá adotar e manter mecanismos de segurança e prevenção, técnicos e administrativos aptos a proteger os dados pessoais compartilhados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, obrigando-se a proceder às adequações demandadas pela CONTRATANTE com o fim de resguardar a segurança e o sigilo dos dados.

14.8. A CONTRATADA e a CONTRATANTE deverão registrar todas as atividades de tratamento de dados pessoais realizadas em razão deste CONTRATO.

14.9. A CONTRATADA deverá comunicar a CONTRATANTE, por meio do fiscal do contrato e no prazo máximo de 24 horas da ciência do fato, a ocorrência de qualquer situação que possa acarretar potencial ou efetivo risco ou dano aos titulares dos dados pessoais, e/ou que não esteja de acordo com os protocolos e normas de proteção de dados pessoais.

14.10. A CONTRATADA deverá colocar à disposição da CONTRATANTE todas as informações e documentos necessários para demonstrar o cumprimento das obrigações estabelecidas nesta SEÇÃO, permitindo e contribuindo, conforme conveniência e oportunidade da CONTRATANTE, para eventuais auditorias conduzidas pela CONTRATANTE ou por quem por esta autorizado.

CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15.1. Incumbirá à CONTRATANTE divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA SEXTA – DISPOSIÇÕES FINAIS

16.1. Nenhuma tolerância das partes quanto à falta de cumprimento de qualquer das cláusulas deste contrato poderá ser entendida como aceitação, novação ou precedente.

16.2. Todas as comunicações, avisos ou pedidos, sempre por escrito, concernentes ao cumprimento do presente contrato, serão dirigidos aos seguintes endereços:

CONTRATANTE: Rua Líbero Badaró, nº 190 – Edifício Othon – 17º andar, CEP 01008-000, Centro, São Paulo/SP.

CONTRATADA: _____

16.3. Fica a CONTRATADA ciente de que a assinatura deste termo de contrato indica que tem pleno conhecimento dos elementos nele constantes, bem como de todas as condições gerais e peculiares de seu objeto, não podendo invocar qualquer desconhecimento quanto aos mesmos, como elemento impeditivo do perfeito cumprimento de seu objeto.

16.4. A Administração reserva-se o direito de executar através de outras contratadas, nos mesmos locais, serviços distintos dos abrangidos na presente contratação.

16.5. A CONTRATADA deverá comunicar à CONTRATANTE toda e qualquer alteração nos dados cadastrais, para atualização, sendo sua obrigação manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

16.6. No ato da assinatura deste instrumento foram apresentados todos os documentos de regularidade fiscal e trabalhista, conforme solicitado neste contrato.

16.7. O presente ajuste, o recebimento de seu objeto, suas alterações e rescisão obedecerão a Lei Federal n° 14.133/21 e ao Decreto 62.100/22 e demais normas pertinentes, aplicáveis à execução dos serviços e especialmente aos casos omissos.

16.8. Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

CLÁUSULA DÉCIMA SÉTIMA– FORO (art. 92, §1º)

17.1. Fica desde logo eleito o Foro da Comarca da Capital – Vara da Fazenda Pública - para dirimir quaisquer controvérsias decorrentes do presente certame ou de ajuste dele decorrente.

E para firmeza e validade de tudo quanto ficou estabelecido, lavrou-se o presente termo de contrato, o qual depois de lido e achado conforme, vai assinado e rubricado pelas partes contratantes e duas testemunhas presentes ao ato.

LOCAL E DATA

_____

Representante legal da CONTRATANTE

_____

Representante legal da CONTRATADA

TESTEMUNHAS:

1-

2-

CIDADE DE SÃO PAULO
FAZENDA

TERMO DE REFERÊNCIA
Lei nº 14.133, de 1º de abril de 2021
SERVIÇOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO-DE-OBRA – LICITAÇÃO

Processo Administrativo SEI nº 6017.2023/0033846-3

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO (art. 6º, XXIII, "a" da Lei n. 14.133/2021).

1.1. Contratação de serviços de Segurança da Informação (SOC **–** *Security Operations Center*)**,** nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	1. Serviço de gestão de vulnerabilidades		Qtd
1	Especificação	Medição	Unidades
	Aplicações Web	URL	154
	Ativos de Rede	Ips/Dispositivos	2.208
	Containers	Imagem de Container	130
ITEM	**2. Serviço de monitoramento de ataques cibernéticos**		**Qtd**
2	Tipo	Medição	Unidades
	Correlacionamento de pacotes	EPS	4.000
	Detecção e resposta em Endpoint	Dispositivo	2.059
ITEM	**3. Serviço de respostas aos incidentes de segurança e de privacidade**		**Qtd**
3	Tipo	Medição	Unidades
	Resposta Incidentes	Valor Mensal	1
ITEM	**4. Serviço de inteligência aplicado à segurança**		**Qtd**
4	Tipo	Medição	Unidades
	Monitoramento	Valor Mensal	1
ITEM	**5. Serviços de Teste de Invasão**		**Qtd**
5	Tipo	Medição	
	Reserva de Horas	Hora Homem	50
ITEM	**6. Serviços técnicos especializados**		**Qtd**
6	Tipo	Medição	
	Reserva de Horas	Hora Homem	50

1.1.1. Especificação detalhada do objeto:

OBSERVAÇÃO: Por motivos de didática e facilidade de leitura o item 1.1.1 terá numeração própria (internamente)

1. INTRODUÇÃO

Com o presente processo licitatório, objetiva-se a contratação de empresa especializada em serviços relacionados à temática de Segurança da Informação, principalmente no que diz respeito à definição, operação, monitoramento e uso de ferramentas para prevenção, detecção e resposta a eventos e incidentes de Segurança da Informação, no ambiente tecnológico da Secretaria da Fazenda do município de São Paulo, mais precisamente, o que segue:

- Serviço de gestão de vulnerabilidades;
- Serviço de monitoramento de ataques cibernéticos;
- Serviço de respostas aos incidentes de segurança e de privacidade;
- Serviço de inteligência aplicada à segurança;
- Serviço de teste de invasão (PENTEST);
- Serviços técnicos especializados.

1.1. JUSTIFICATIVA E ALINHAMENTO AO PLANO DIRETOR DE TI

Enquanto órgão arrecadador da Prefeitura de São Paulo, é de relevante importância o zelo e proatividade em evitar que incidentes de segurança da informação possam comprometer o fornecimento de serviços ao público interno/externo, bem como gestão da receita e do tesouro municipal, realizados por meio de sistemas de informação. Paralelamente, a Lei Geral de Proteção de Dados adiciona novos elementos que destacam ainda mais a necessidade pelo cuidado no tratamento de dados pessoais e/ou dados sensíveis/sigilosos.

De tal forma, e, principalmente, tendo em vista diversos casos de incidentes de segurança da informação (exemplos a seguir), justifica-se a contratação dos serviços descritos no presente Termo de Referência.

https://www.band.uol.com.br/rio-de-janeiro/noticias/site-nota-carioca-volta-a-funcionar-depois-de-nove-dias-16530386

https://oglobo.globo.com/rio/noticia/2022/09/invasao-hacker-obrigara-prefeitura-a-trocar-ate-20-mil-computadores.ghtml

https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx

https://agenciabrasil.ebc.com.br/economia/noticia/2022-09/banco-central-comunica-vazamento-de-dados-de-1373-mil-chaves-pix

1.2. RESULTADOS ESPERADOS

Diante dos serviços elencados, é esperado que o ambiente tecnológico da Secretaria, bem como os dados (especialmente os pessoais/sensíveis/sigilosos), sistemas e serviços prestados ao público interno/externo, como também a arrecadação e a gestão do tesouro, estejam ativa e passivamente protegidos de ameaças, com riscos, vulnerabilidades conhecidos, registrados e endereçados, de forma a evitar danos decorrentes de vazamentos, fraudes e/ou indisponibilidade e/ou inadequação nos acessos aos sistemas.

2. CONSIDERAÇÕES GERAIS

2.1. A prestação do serviço compreende a operação contínua e cotidiana das ferramentas e mecanismos de segurança da informação e, principalmente, situações reais de emergência, crise, ataques, vazamentos de informações e eventos correlatos.

2.2. No advento das situações acima exemplificadas, a CONTRATADA deve ter total protagonismo no combate, mitigação, resolução da ameaça e danos decorrentes.

2.3. A CONTRATANTE tem a prerrogativa de declarar situações de crise e classificar, reclassificar eventos/incidentes.

2.4. Os objetivos descritos, para cada serviço (**Item 3** da **Especificação detalhada do objeto (1.1.1)**) precisam ser atendidos em sua respectiva plenitude.

2.5. As ferramentas, sempre que possível, deverão alimentar o console do **Serviço de resposta aos incidentes de segurança/privacidade** (**Item 3.3** da **Especificação detalhada do objeto (1.1.1)**), a partir de onde o ciclo de vida dos eventos será monitorado.

2.6. A alocação da mão de obra utilizada e dimensionamento da equipe necessária se dará a critério da CONTRATADA, atendidas as disposições deste Termo de Referência, principalmente no que diz respeito ao Acordo de Nível de Serviço (ANS/SLA).

2.6.1. Para garantir a continuidade e atendimento aos serviços prestados, cabe à CONTRATADA observar o impacto de férias e outras ausências trabalhistas que possam afetar a correta prestação do serviço/ atendimento aos respectivos prazos e ANS.

2.7. O preposto será o representante da CONTRATADA para fins da prestação objeto deste termo de referência e será o interlocutor da CONTRATADA com a CONTRATANTE.

2.7.1. A CONTRATADA deverá indicar formalmente o preposto ao Gestor do Contrato, em correspondência encaminhada com cópia ao Fiscal do Contrato, ambos da CONTRATANTE e deverá comunicar a sua alteração ou substituição sempre que necessário.

2.8. A CONTRATADA, além do preposto, deverá indicar gerentes para cada um dos serviços prestados (**Item 3** da **Especificação detalhada do objeto (1.1.1)**):

2.8.1. O perfil dos gerentes indicados deve obedecer ao disposto em Perfil Profissional (**Item 12** da **Especificação detalhada do objeto (1.1.1)**).

2.8.2. Em situações emergenciais, ou a critério da CONTRATANTE, todos os gerentes podem ser requisitados a comparecer presencialmente nas dependências da CONTRATANTE (**Itens 2.9, 2.11** e **2.15** da **Especificação detalhada do objeto (1.1.1)**).

2.8.3. O prazo para apresentação é de 24h a contar da convocação, não afastando a urgência e o atendimento remoto imediato e independe da qualidade de ser dia útil ou não.

2.8.4. Dentro do escopo dos serviços elencados, os profissionais indicados pela CONTRATADA podem, atendidos os requisitos do **Item 2.8.1** supra, acumular as gerências dos serviços.

2.8.5. Em caso de acúmulo de gerência por um mesmo profissional, além dos aspectos técnicos e de perfil (**Item 2.8.1** supra), o **Acordo de Nível de Serviços** ((**Item 8** da **Especificação detalhada do objeto (1.1.1)**) deve ser observado.

2.9. O datacenter principal da CONTRATANTE está localizado no Edifício Othon, na Rua Líbero Badaró, nº 190, Primeiro Subsolo - Centro, São Paulo - SP, doravante denominado datacenter. A CONTRATANTE poderá criar outros datacenters, extensões, alterar a localização ou excluir os mesmos;

2.10. Em caso de alteração da localização, criação de novos datacenters, criação de extensões ou exclusão destes, a CONTRATANTE deverá comunicar, à CONTRATADA, sobre o início das operações na nova localidade com, no mínimo, 60 dias de antecedência;

2.11. São extensões do datacenter principal as unidades:

2.11.1. Controle Direto:

- Gabinete - Vd. Do Chá, 15 - Ed. Matarazzo – Centro;
- Nuvem.

2.11.2. Controle Indireto:

- PRODAM Barra Funda: Av. Francisco Matarazzo, 1.500 - Ed. Los Angeles Água Branca;
- PRODAM Pedro de Toledo, PRODAM - R Pedro de Toledo 983 - Vila Clementino.

2.12. O núcleo de operações e controle (NOC) da CONTRATANTE está localizado no Edifício Othon, na Rua Líbero Badaró, nº 190, Centro, São Paulo - SP.

2.13. O SOC – *Security Operations Center*, objeto principal do presente Termo de Referência, compreende o serviço contratado, o corpo profissional da CONTRATADA, os profissionais da CONTRATANTE envolvidos direta ou indiretamente com o objeto deste Termo de Referência, em regime de trabalho/operações presencial ou remoto.

2.14. As informações da CONTRATANTE deverão ser armazenadas unicamente nos locais definidos pela CONTRATANTE.

2.15. São dependências da CONTRATANTE:

- Edifício Matarazzo, localizado no Viaduto do Chá, número 15, Anhangabaú, São Paulo - SP;
- Edifício Othon, localizado na Rua Líbero Badaró, nº 190, Centro, São Paulo – SP.

2.16. A CONTRATADA deve observar o **Item 5 Transição de Serviços e Conhecimento** da **Especificação detalhada do objeto (1.1.1)**, que apresenta fases de recepção do ambiente e transição de serviços, instruindo como deverá recepcionar os serviços, bem como quais documentos deve manter e entregar ao final do Termo Contratual.

2.17. As especificações técnicas dos serviços a serem ofertados referentes ao objeto, devem ser interpretadas de forma a melhor atender aos objetivos especificados nos respectivos serviços.

2.18. O ambiente tecnológico da CONTRATADA, pode ser verificado no **Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**.

2.19. Para o início da execução contratual uma ou mais Ordens de Serviço poderão ser emitidas, de forma a delimitar com precisão o objeto, os custos e os prazos da execução do serviço-alvo da respectiva Ordem de Serviço (OS).

2.20. É responsabilidade da CONTRATADA a utilização, a instalação, a configuração e a manutenção da solução (ainda que em formato *on-premise)*, bem como licenças, adaptações acessórias, equipamentos e insumos acessórios à prestação do serviço.

2.21. É responsabilidade da CONTRATANTE a disponibilização de elementos estruturais e pressupostos básicos (notadamente fora do escopo do serviço), mas imprescindíveis para tal, tais como para o funcionam do espaço físico, energia elétrica e link de internet.

2.21.1. Insumos de instalação, tais como ferramentas, fiação, mão de obra básica e congêneres, necessários para interligar a estrutura da CONTRATANTE ao serviço prestado pela CONRATADA, será de responsabilidade da CONTRATADA.

2.21.2. Sempre que necessário, deverão fazer parte do fornecimento os servidores físicos necessários, obedecendo as especificações mínimas recomendadas pelo fabricante, assim como sistemas operacionais, sistemas de virtualização e softwares complementares para a completa instalação do sistema, atendendo a todas as características solicitadas, podendo a contratante ceder espaço de alocação no datacenter mediante prévia análise.

2.22. Todos os softwares não podem constar, no momento da apresentação da proposta técnica, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida.

2.23. Deve-se englobar a alocação de softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

2.24. Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada, e estarem cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os softwares fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante/mantenedor.

2.25. Não deve haver incompatibilidade dentre as soluções tecnológicas fornecidas pela CONTRATADA.

2.26. As soluções devem possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console.

2.27. A CONTRATADA deve adotar configuração de servidor NTP para sincronização de relógios dos componentes das soluções fornecidas.

2.28. A CONTRATADA não se obriga a consumir nenhum dos quantitativos estipulados no **Item 4 Expectativa de Consumo** da **Especificação detalhada do objeto (1.1.1).**

2.29. Para aqueles itens em que a medição é realizada por critérios quantitativos, tal valor será estipulado em uma ou mais Ordem de Serviço.

2.30. Para fins de faturamento de determinado período contratual, a quantidade a ser utilizada no cômputo da fatura será a quantidade presente na prestação de cada serviço no último dia do ciclo de faturamento em questão.

2.31. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

2.32. A fim de mitigar e prever possíveis impactos na infraestrutura da CONTRATANTE, antes do início da execução dos serviços, as ferramentas adotadas para execução deverão ser apresentadas ao time de segurança da informação da CONTRATANTE, que poderá ou NÃO aprovar a utilização das mesmas.

2.33. As soluções devem ser capazes de produzir relatórios nos seguintes formatos: PDF, CSV e HTML.

2.34. Custos acessórios, tais como deslocamento e/ou hospedagem, de profissionais da CONTATADA, serão custeadas pela mesma.

2.35. As soluções (inclusive relatórios e dashboards), que se utilizem de determinados scores (exemplificativamente CVSS), devem ranquear e/ou ponderar tais indicadores considerando relevância e priorização de segurança dos ativos no contexto do ambiente tecnológico e regras da CONTRATANTE, a fim de considerar o real impacto no negócio.

2.36. Os integrantes do SOC não deverão ter acesso com permissões de administrador à infraestrutura/NOC. Sendo necessária, portanto, a abertura de chamados ao outro contrato, para que configurações sejam efetivadas.

2.37. Os integrantes do SOC, sempre que necessário, deverão participar das reuniões e aprovações de mudanças na infraestrutura da contratada.

2.38. Sempre que necessário, deverão acontecer reuniões presenciais entre equipes do NOC e SOC.

2.39. Levando-se em consideração que muitos dos serviços aqui descritos são de alta criticidade, em termos de segurança de dados, eventuais serviços, que já estejam cobertos por outros contratos, somente serão utilizados pelo objeto contratual aqui descrito, quando do encerramento dos outros contratos.

2.40. A CONTRATANTE deverá ter acesso a todos os sistemas envolvidos na prestação do serviço.

3. DO SERVIÇOS CONTRATADOS

3.1. Serviço de gestão de vulnerabilidades:

3.1.1. Descrição: varredura ativa de vulnerabilidades de todos os itens (aplicações ou ativos de rede, containers) definidos pela CONTRATANTE, mediante Ordem de Serviço. A solução de varreduras adotada pela CONTRATADA, deverá ser capaz de analisar toda a infraestrutura de TI (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**), conforme descritivos e quantitativos informados.

3.1.2. Objetivo a ser atingido: identificar, de forma proativa e recorrente, possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da CONTRATANTE, com o intuito de evitar que ataques cibernéticos sejam realizados com sucesso contra o ambiente da CONTRATANTE. O serviço também contempla a gestão de vulnerabilidade e seus respectivos atributos.

3.1.3. Medição: o serviço será fornecido e medido por meio dos seguintes itens:

3.1.3.1. Aplicações Web: quantidade de URLs monitoradas;

3.1.3.2. Ativos de Rede: quantidade de IPs e/ou Dispositivos monitorados;

3.1.3.3. Container: quantidade destes objetos.

3.1.4. Processo de identificação e gestão de vulnerabilidades:

A CONTRATANTE apresentará, em sendo o caso, mediante visitas presenciais, dados acerca do ambiente tecnológico, demais informações necessárias para a prestação do serviço.

A CONTRATADA deverá proativamente sugerir inclusão ou exclusão de itens tomando por base o **Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**, bem com as visitas presenciais.

A CONTRATADA deverá apresentar inicialmente um **Plano de Identificação e Gestão de Vulnerabilidades (Item 3.1.6.1 abaixo)**, indicando, os ativos, as ferramentas e as técnicas que visem atingir ao objetivo descrito no item **3.1.2** supra, e ainda como deverão ser gerenciados os eventos/incidentes em ferramenta de gestão proposta pela CONTRATADA.

A CONTRATANTE emitirá Ordem de Serviço, aprovando o plano apresentado.

A CONTRATADA realizará de forma contínua e proativa varreduras, em busca de vulnerabilidades.

Após término de cada rotina, a CONTRATADA deve realizar uma análise de falso positivo e apresentar à CONTRATANTE apenas vulnerabilidades legítimas, bem como orientações de como atuar acerca das mesmas.

Após término de cada rotina, a CONTRATADA deve realizar uma análise melhorias a serem implementadas no processo de varredura de vulnerabilidades, sempre buscando atingir o objetivo anteriormente descrito.

3.1.5. Interface com demais serviços: sempre que possível, as interfaces entre serviços devem operar de forma integrada, de forma atingir os respectivos objetivos descritos.

3.1.6. Entregáveis:

A CONTRATADA deve entregar mensalmente ou quando solicitada:

3.1.6.1. **Plano de Identificação e Gestão de Vulnerabilidades** (em sendo o caso de atualizações), contendo diagrama didático e atualizado da estrutura dos ativos, ferramentas e técnicas de varredura;

3.1.6.2. Relatório contendo informações importantes e pertinentes acerca das vulnerabilidades, tais como:

- Data detecção da vulnerabilidade
- Id no sistema de monitoramento
- Tipo de Vulnerabilidade
- Severidade
- Área Responsável
- Ativo alvo específico
- Categoria do Alvo: Aplicação Web; Dispositivo; Container
- Demais atributos que a CONTRATANTE/CONTRATADA possam sugerir.

3.1.7. Referência ao SLA: ver o **Acordo de Nível de Serviços** (**Item 8** da **Especificação detalhada do objeto (1.1.1)**)

3.1.8. Especificações técnicas:

As especificações técnicas são como balizas para a definição de requisitos do serviço, mas que devem ser interpretadas sempre de forma a possibilitar o alcance do objetivo definido (**Item 3.1.2** supra).

As ferramentas e soluções utilizadas para prestação do serviço supracitado deverão possuir características de:

- **Descoberta de vulnerabilidades**: soluções e/ou ferramentas fornecidas e utilizadas pela CONTRATADA para realizar o processo de descoberta de novas vulnerabilidades de aplicações, infraestrutura e containers.
- **Gestão de vulnerabilidades**: soluções e/ou ferramentas fornecidas e utilizadas pela CONTRATADA para gerir todo o ciclo de vida das vulnerabilidades encontradas, desde a sua descoberta até sua correta mitigação.

Independente do grupo das soluções supracitadas, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir todos os requisitos previstos no **Item 2.**

CONSIDERAÇÕES GERAIS da **Especificação detalhada do objeto (1.1.1)** e podem ser prestados por meio de solução instalada *on-premise* ou provida através da nuvem do fabricante ou da CONTRATADA.

3.1.8.1. Descoberta de Vulnerabilidades:

A CONTRATADA deverá compor ao ambiente de segurança, solução de descoberta de vulnerabilidades capaz de identificar vulnerabilidades de infraestrutura e aplicações que possam comprometer a disponibilidade, integridade e confiabilidade dos dados e serviços da CONTRATANTE.

As soluções de prestação dos Serviços de Gestão de Vulnerabilidades deverão estar disponíveis para serem acessadas, além da própria CONTRATADA, também pela CONTRATANTE, caso essa julgue ser necessário, de modo a prover varredura, identificação e gestão de vulnerabilidades do parque computacional.

Deverá ser utilizada ferramenta de análise de vulnerabilidade com foco em infraestrutura, em aplicações web e em containers/camadas de virtualização.

A CONTRATADA também deve utilizar, além de ferramentas, métodos e técnicas assistidas, para identificar possíveis vulnerabilidades, com o intuito de atingir os objetivos especificados no **Item 3.1.2** supra.

A solução deve possibilitar varreduras (*scans*) de vulnerabilidades, avaliação de configuração e conformidade (*baseline* e *compliance*) e indícios e padrões de códigos maliciosos conhecidos (*malware*).

A solução deve possuir recurso de varredura ativa, onde o *scanner* comunica-se com os alvos (ativos) através da rede.

A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões, e gerenciar todos por uma console central.

O serviço deve possibilitar, inclusive por meio por meio da console, que a atividade de varredura atinja toda a rede, indiferente do método de escaneamento, que poderá ser:

- *Scan* ativo;
- *Scan* com uso de agentes;
- *Scan* passivo.

A solução deverá fornecer funções de priorização de varreduras, a serem estipuladas *ad-hoc*, pela CONTRATANTE e CONTRATADA, conjuntamente.

Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades, incluindo feeds de inteligência de ameaças ao vivo.

A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional.

A solução deve possuir conectores para as principais plataformas cloud (Amazon Web Services, Microsoft Azure, Google Cloud) e, principalmente, sempre que aplicável, ser compatível com os ativos previstos no **Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1).**

Cabe à CONTRATADA, no advento do certame licitatório, analisar o item (Ambiente Tecnológico) para garantir que a proposta e eventual prestação de serviço seja eficaz.

A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados.A quantidade de scanners ativos e sensores passivos deverá contemplar o monitoramento da integralidade do ambiente (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**) da CONTRATANTE, de forma a atingir os objetivos descritos em **Item 3.1.2** supra.

Deve ser possível determinar em tempo real, quais portas estão abertas em determinado ativo.

Deve ser capaz de guardar, no mínimo, os seguintes atributos de um ativo:

- MAC Address;
- Nome NetBIOS;
- FQDN.

A solução deve ser capaz de realizar - em tempo real - a descoberta de novos ativos para, no mínimo:

- Bancos de dados;
- *Hypervisors*;
- Dispositivos móveis;
- Dispositivos de rede;
- *Endpoints*;
- Aplicações.

Deve realizar - em tempo real - a identificação de informações sensíveis no tráfego de rede do ambiente.

A solução deve ser capaz de identificar a comunicação de *malwares* na rede, de forma passiva.

Deve ter a capacidade de guardar - em tempo real - informações de GET, POST e Download que trafeguem na rede;

A solução deve ser capaz de - em tempo real - detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;

Permitir identificar vulnerabilidades associadas aos servidores SQL no tráfego de rede - em tempo real - sem a necessidade de um agente;

A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo, no mínimo, Windows, Linux e Mac OS, bem como *appliances* virtuais, em especial, aqueles previstos no **Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**;

A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de configurações e vulnerabilidades.

A solução deve incluir a capacidade de programar períodos de tempo e data em que varreduras não podem ser executadas, como, por exemplo, em determinados dias do mês ou determinados horários do dia.

No caso em que uma atividade de varredura for interrompida por invadir o período não permitido, a mesma deve ser capaz de ser reiniciada de onde parou.

A solução deve ser configurável para permitir a otimização das configurações de varredura.

A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux.

A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até o acesso de sistema ou administrativo.

Deve ser capaz de estimar a criticidade dos ativos da organização.

A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE, comparando sua maturidade com outras organizações, padrões ou boas práticas definidas;

Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo).

A solução deve gerar uma pontuação global referente a exposição cibernética da organização, baseada nas pontuações de cada um dos ativos.

A solução deve permitir um acompanhamento histórico do nível de exposição da organização.

Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução.

A solução deve permitir a segregação lógica entre áreas distintas da empresa, a fim de obter a pontuação referente a exposição cibernética por área.

3.1.8.2. Gestão de Vulnerabilidades:

O serviço deverá incluir um console unificado, que integre os demais sistemas/ferramentas do presente objeto, apresentando o ciclo da vulnerabilidade, incidentes e/ou ativos monitorados, respectivos logs de eventos/auditoria, bem como informações correlatas ao objeto deste edital.

O console, sempre que possível irá comunicar-se, via API, com ferramentas dos demais serviços previstos no presente documento.

O console deverá ser acessível ao pessoal do quadro da CONTRATANTE, mediante *Microsoft Active Directory*.

3.1.8.3. Requisitos de segurança

A solução deve criptografar todas as informações em trânsito.

Deve ser capaz de criptografar os dados armazenados.

A solução deve ser capaz de gerar uma chave randômica com no mínimo 256 bits para cada scanner conectado na plataforma de gerência.

Todos os dados enviados para a plataforma de gerenciamento devem ser criptografados – no mínimo – com protocolo TLS 1.3, com tamanho de chave de 4096 bits.

A solução deve possuir ferramentas e processos automatizados para monitorar: *Uptime*, Comportamentos anômalos e performance da plataforma.

Deve possuir retenção de – no mínimo – 12 meses dos resultados dos *scans* realizados no ambiente.

3.1.8.4. Varreduras de aplicações web

A solução deve realizar varreduras de vulnerabilidades em aplicações Web, cobrindo, no mínimo, mas não se limitando, a base de ameaças apontadas pelo OWASP Top 10.

A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web, como parte dos ativos a serem inspecionados.

A solução deverá ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS).

Para varreduras extensas e detalhadas, deve varrer e auditar – no mínimo – os seguintes elementos:

- Cookies, Headers, Formulários e Links;
- Nomes e valores de parâmetros da aplicação;
- Elementos JSON e XML;
- Elementos DOM.

Deverá também permitir somente a execução da função *crawler*, que consiste na navegação para descoberta das URLs existentes na aplicação.

Deve ser capaz de utilizar *scripts* customizados de *crawl*, com parâmetros definidos pelo usuário.

Deve ser capaz de excluir determinadas URLs da varredura, através de expressões regulares.

Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões.

Deve ser capaz de instituir – no mínimo – os seguintes limites:

- Número máximo de URLs para *crawl* e navegação;
- Número máximo de diretórios para varreduras;
- Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
- Número máximo de requisições HTTP por segundo.

Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual.

Deve suportar o envio de notificações por e-mail.

Deverá ser compatível com avaliação de *web services* REST e SOAP.

A solução deve suportar os seguintes esquemas de autenticação:

- Autenticação Básica (Digest);
- NTLM;
- Autenticação de Cookies;
- Autenticação através de Selenium.

Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário.

Deve ser capaz de customizar parâmetros Selenium como: delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos.

A solução deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades.

Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações.

Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências.

Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação.

A solução deve ser capaz de realizar varreduras no ambiente tecnológico da CONTRATANTE (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**)

3.1.8.5. Relatórios

Deve ser capaz de executar relatórios manuais e periódicos de acordo com a frequência estabelecida pelo administrador;

A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

A solução deve suportar o envio automático de relatórios para destinatários específicos;

Deve ser possível definir a frequência na geração dos relatórios para, no mínimo: Diário, Semanal, Mensal e Anual;

Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

A solução deve possuir relatórios pré-configurados com as seguintes informações:

- *Hosts* verificados sem credenciais;
- Top 100 Vulnerabilidades mais críticas;
- Top 10 *Hosts* infectados por *Malwares*;
- *Hosts* exploráveis por *Malwares*;
- Total de vulnerabilidades que podem ser exploradas pelo *Metasploit*;
- Vulnerabilidades críticas e exploráveis;
- Máquinas com vulnerabilidades que podem ser exploradas;
- Relatórios contendo *scans* credenciados que tiveram erro ou falha.

A solução deve possuir *dashboards* customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;

Deve possuir *dashboard* apresentando visão das vulnerabilidades discriminadas por sua criticidade e idade.

3.2. Serviço de monitoramento de ataques cibernéticos:

3.2.1. Descrição: monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao ambiente definido pela CONTRATANTE, mediante solução de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura.

3.2.2. Objetivo a ser atingido: registro e tratamento de eventos de segurança da informação, os quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo a um processo cíclico e rigoroso de gestão de eventos.

3.2.3. Medição: o serviço será fornecido e medido por meio dos seguintes itens:

3.2.3.1. Correlacionamento de Pacotes: quantidade de Eventos por Segundo (EPS):

- A solução deverá monitorar uma quantidade de EPS definida por Ordem de Serviço e com a obrigação de suportar picos que excedam o quantitativo estipulado por até 8 dias no ciclo mensal de faturamento.

3.2.3.2. Detecção e resposta em *endpoints*: quantidade de Dispositivos monitorados.

3.2.4. Processo de monitoramento de ataques cibernéticos:

A CONTRATANTE apresentará, em sendo o caso, mediante visitas presenciais, dados acerca do ambiente tecnológico, demais informações necessárias para a prestação do serviço.

A CONTRATANTE deverá proativamente sugerir inclusão ou exclusão de itens tomando por base o disposto no **Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)** e dados coletados nas visitas presenciais.

A CONTRATADA deverá apresentar um **plano de monitoramento e linha base de eventos monitorados**, bem como ferramentas e técnicas que visem atingir ao objetivo descrito no **Item 3.2.2** supra.

A CONTRATANTE emitirá Ordem de Serviço, aprovando o plano apresentado.

Sempre que necessário, ajustes nos eventos monitorados poderão ser solicitados, dentro dos termos e quantitativos contratuais.

A CONTRATADA opera a ferramenta de forma a correlacionar os pacotes e identificar eventos.

A CONTRATADA não deve apenas deixar o correlacionamento exclusivamente a cargo das ferramentas, mas ser proativa de forma a tornar o uso da ferramenta o mais eficaz possível e atingir os objetivos elencados.

Os eventos devem ser classificados em:

- **EVENTOS DE INFORMAÇÃO**: possuem a finalidade de verificar o funcionamento dos itens de configuração de segurança e de fornecer estatísticas.
- **EVENTOS DE AVISO**: devem ocorrer em face a comportamentos anômalos, tomando por referência a linha de base anteriormente definida.

- **EVENTOS DE EXCEÇÃO**: indício de que algum elemento de segurança foi burlado e demanda urgente atenção/resposta.

Os registros devem ser mantidos em sistema de gestão de eventos, a partir do qual relatórios e acompanhamento do ciclo de vida do evento possam ser comunicados, analisados e monitorados.

Após a detecção e registro do evento passa-se às tarefas de adequada resposta aos mesmos.

3.2.5. **Interface com demais serviços**: sempre que possível, as interfaces entre serviços devem operar de forma integrada, de forma atingir os respectivos objetivos descritos.

3.2.6. **Entregáveis**:
A CONTRATADA deve entregar mensalmente ou quando solicitada:

3.2.6.1. Plano de Monitoramento contendo um diagrama didático e atualizado da estrutura e ferramentas de varredura

3.2.6.2. Relatório em formatos (PDF, CSV e HTML) contendo informações acerca dos eventos registrados e pelo menos os seguintes atributos, de forma que filtragens, gráficos e/ou cruzamentos possam ser efetuados.

3.2.6.3. Quantitativo de eventos registrados com as seguintes informações correlatas:

- Data do evento
- Id no sistema de monitoramento
- Tipo de Vulnerabilidade
- Tipo de Ataque
- País de Origem
- IPs
- Tipo de Evento
- Regra de Correlacionamento
- Severidade
- Área Responsável
- Ativo alvo específico
- Categoria do Alvo: Aplicação Web; Dispositivo; Container
- Demais atributos que a CONTRATANTE/CONTRATADA possam sugerir.

3.2.6.4. Relatórios diversos fornecidos pela solução de varredura em *endpoint*.

3.2.7. **Referência ao SLA**: ver o **Acordo de Nível de Serviços** (**Item 8** da **Especificação detalhada do objeto (1.1.1)**)

3.2.8. **Especificações técnicas**:

As especificações técnicas são como balizas para a definição de requisitos do serviço, mas que devem ser interpretadas sempre de forma a possibilitar o alcance do objetivo definido (**Item 3.2.2** supra).

3.2.8.1. Correlacionamento de Logs

Todos os módulos que compõem a solução deverão se integrar visando constituir um ambiente conjunto de análise, investigação, inteligência, defesa cibernética e resposta a incidentes nos processos, incluindo má utilização dos sistemas e tentativas sequenciais de utilização suspeitas, inclusive, entre sistemas e plataformas diferentes.

A solução deverá fornecer, pelo menos: módulo de coleta de pacotes e logs e geração de metadados, módulo de indexação, agregação e enriquecimento dos metadados dos coletores, módulo de correlacionamento avançado de alertas e tratamento de incidentes, e módulo de gerência centralizada de todos os outros módulos envolvidos.

Possuir arquitetura distribuída para captura de logs, fluxos de rede, tráfego de rede, e toda a análise de forma centralizada de todos os tipos de capturas.

Implementar comunicação criptografada entre todos os componentes envolvidos.

A solução deve ser fornecida com todos os sistemas operacionais e sistemas de gerenciamento de banco de dados necessários para o seu funcionamento.

Caso a solução seja no modelo on-premise, todos os componentes da solução devem suportar no mínimo a instalação no ambiente tecnológico da CONTRATANTE (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**).

Possuir um módulo de monitoração de desempenho e saúde dos componentes envolvidos;

Deverá possuir retenção mínima de 01 (um) ano dos registros de eventos.

Possuir métricas de saúde dos equipamentos como: utilização de CPU, utilização de memória, disco rígido, status do serviço, status das conexões.

Suportar armazenamento externo de logs, fluxos, dados de rede e seus metadados através de Direct-Attached Capacity (DAC) ou Storage Area Network (SAN);

Suportar de forma nativa e automática o arquivamento logs e metadados em camadas com as seguintes funcionalidades: hot (dados online presentes em sistemas de discos rápidos, como SAN e SSD ou similares), warm (dados online presentes em sistemas de discos de alta capacidade, como NAS e discos SAS, NLSAS ou similares) e cold (dados não gerenciados presentes em sistemas de armazenamento offline para possível restauração);

Deve permitir especificar períodos de retenção de dados online (hot e warm) e suportar a compactação e o arquivamento das informações de dados e metadados em área de armazenamento via CIFS/NFS.

Permitir a configuração de perfis de acesso com permissão e restrição ao conteúdo de dados e metadados de eventos, logs, auditoria de operação e administração da solução, além de se integrar com os recursos de autenticação e autorização suportando, no mínimo, Microsoft Active Directory.

Implementar Single Sign-On.

Possuir controle de acesso baseado em perfis de usuários.

Possuir serviço de monitoração de estado de recebimento e processamento de logs e eventos.

A solução deve ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos.

Ser capaz de notificar o administrador automaticamente caso a quantidade de eventos de algum dispositivo monitorado exceda limiares (acima e abaixo) de taxa de eventos.

Permitir a administração a partir da console de gerência de todos os componentes da solução, incluindo suas configurações, instalação e ativação de módulos e componentes, monitoramento de utilização de recursos (CPU e memória) e logs dos próprios componentes.

A solução deve possuir função de verificação/atualização de software e conteúdo de bases de vulnerabilidades ou informações correlatas de segurança da informação, de forma automática, com notificação visual na interface de administração da ferramenta.

Implementar a verificação de atualizações de software e conteúdo disponíveis de forma automática com notificação visual na interface de administração e download.

A solução deve suportar o recebimento e interpretação de eventos no formato Common Event Format (CEF).

Implementar capacidade de coletar e interpretar logs dos principais sistemas operacionais, em especial aqueles previstos no ambiente tecnológico da CONTRATANTE (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**).

Implementar capacidade de coletar e interpretar logs de firewalls, antivírus, IDSs, proxies, servidores web, servidores DNS, balanceadores de carga, roteadores, switches e demais dispositivos de rede.

Implementar capacidade de coletar e interpretar logs de IBM zOS e RACF.

Implementar capacidade de coletar e interpretar eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos syslog, syslog NG, SNMP Trap, VMware vCenter API,, AWS (Amazon Web Services) Security Hub, Azure Audit, Azure Active Directory, Sign-in e Management, Azure Network Security Groups (NSG) e Office 365 Management Activity API.

Implementar capacidade de coletar logs dentro da infraestrutura de nuvem pública, devendo os dados transmitidos serem compactados e criptografados.

Implementar capacidade de coletar e interpretar logs de soluções de firewall de aplicação (WAF) como o Apache Mod Security e aqueles previstos no ambiente tecnológico da CONTRATANTE (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**)

Implementar capacidade de coletar e interpretar logs de soluções de versionamento de código, incluindo as ferramentas GitHub Enterprise e Microsoft Team Foundation Server.

Implementar capacidade de coletar e interpretar logs no formato JSON;

Ser capaz de receber logs e eventos oriundos de um relay de syslogs.

Ser capaz de receber logs de ferramentas de avaliação de vulnerabilidade.

Permitir a criação de novos interpretadores de eventos e logs.

Possuir uma ferramenta gráfica, integrada a solução, para criação de interpretadores para dispositivos ou eventos não suportados nativamente.

Permitir a utilização ou a criação de mecanismos complexos para captura de logs como, por exemplo, realizar o download via HTTPS de um arquivo compactado de logs armazenados em um servidor web, descompactar e extrair os logs.

Permitir a importação manual de arquivos de logs.

Possuir a capacidade de identificação do tráfego de rede capturado na interface de rede através da captura de pacotes, com reconhecimento nativo de protocolos e aplicações.

Deve ser compatível com soluções de packet brokers e de inspeção SSL e TLS para captura de tráfego descriptografado.

Permitir a captura de pacotes em ambientes de nuvem pública, suportando, pelo menos, Amazon Web Services (AWS) (VPC Traffic Mirror) e Microsoft Azure, e nuvem privada, suportando, pelo menos, VMware.

Possuir a capacidade de identificação de sessões de TeamViewer, VNC e X11.

Possuir a capacidade de identificação de túneis Teredo.

Possuir a capacidade de identificação de fabricantes de interfaces de rede a partir do Ethernet OUI.

Implementar a identificação de perfil tráfego criptografado através do fingerprinting de TLS/SSL, sem a necessidade de importação de chaves privadas.

Possuir a capacidade de extração de informações de sessões TLS incluindo, pelo menos, o subject, número de série, ON (Organizational Name) ou CN (Common Name), a CA (Certificate Authority) de todos os certificados presentes em uma cadeia.

Permitir que seja configurado, se o módulo de coleta de tráfego deve realizar apenas a extração de metadados sem armazenamento do tráfego e o armazenamento do tráfego e a extração de metadados.

O NDR deverá atender a todas as especificações previstas no presente item, inclusive quanto ao processamento de pacotes e identificação de tecnologias, funcionando como mecanismo de resposta ao SIEM e, principalmente, atingir os objetivos definidos.

Suportar a aplicação de regras de filtragem de protocolos.

Suportar a configuração de filtros capazes de excluir partes de pacotes que seriam armazenados.

Suportar a criação de regras de exclusão de capturas baseados em IP de origem, IP de destino, porta de origem e porta de destino.

Suportar decifrar uma sessão de rede criptografada em qualquer protocolo da camada de aplicação da pilha TCP/IP suportado, tendo conhecimento da chave privada de criptografia utilizada na transmissão, sem requerer o uso de soluções externas.

Permitir a importação e exportação de arquivos pcap capturados pelas ferramentas libpcap, WinPcap e Npcap.

Possuir a capacidade de criação de interpretadores para protocolos, aplicações proprietárias e aplicações desconhecidas.

Permitir a criação customizada de interpretadores para identificação de protocolos de rede específicos.

Possuir a capacidade de identificação de protocolo pelo conteúdo das sessões, independente da porta utilizada de comunicação.

Permitir a extração de arquivos presentes no tráfego de rede capturado.

Permitir a reconstrução de imagens e arquivos a partir do tráfego coletado.

Ser capaz de analisar tráfego IPv4 e IPv6.

Possuir painel configurável que permita a rápida visualização da sessão reconstruída, equivalente ao tráfego que gerou o alerta.

Possuir a capacidade de exibir visualmente os objetos trafegados pela rede, sem a necessidade de manipular os dados diretamente na console ou banco de dados.

Permitir exportar e importar arquivos contendo pacotes de tráfego de rede em seu formato bruto, com possibilidade de gerar e verificar a informação de integridade desses arquivos.

Permitir a visualização das sessões nos seguintes formatos: metadado, texto, hexadecimal, pacotes, reconstrução web (HTTP), reconstrução e-mail (SMTP) e arquivos.

Permitir a análise de dados na camada de aplicação (modelo OSI) a partir de entidades como usuários, e-mail, endereço, arquivos e ações.

Permitir a exportação de logs e eventos armazenados nos formatos texto, XML, JSON e CSV.

Permitir a coleta informações de estações de trabalho Windows, Linux e Mac, incluindo arquivos, autoruns, processos, drivers, bibliotecas e informações do sistema.

Implementar a coleta de logs de estações e servidores Windows incluindo, pelo menos, os canais Sistema (System), Segurança (Security), Aplicação (Application).

Deve permitir habilitar e desabilitar a coleta de logs por grupos de estações configurados pelo administrador a partir da console de gerência.

A coleta de logs deve ser realizada utilizando um protocolo seguro e criptografado.

Deve permitir a coleta de tipos de eventos específicos (Event ID).

Implementar gerenciamento de ativos que permita definir atributos tais como nome, descrição, nome no DNS, prioridade, criticidade, localização na rede, sistema operacional, localização geográfica, departamento, contato do responsável pelo ativo, fabricante, número de série, e campos personalizados.

O envio de dados entre os componentes da solução, tais como coletores e concentradores, deve ser com garantia de entrega, a fim de eliminar riscos de perda de informações por problema de rede, ou outros problemas.

Possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos de qualquer meio (logs, fluxos e rede).

Possuir a capacidade de análise avançada de eventos em tempo real, através de regras de correlação e eventos complexos em dados correlacionados.

Permitir controlar um conjunto de regras de correlação que serão aplicadas em eventos processados em determinados concentradores determinados pelo administrador.

Implementar notificação através de alertas de comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período.

Permitir a criação e customização de regras na própria interface, com uma ferramenta que permita testes da regra com eventos.

Permitir a criação e customização de regras de incidentes na própria interface.

Permitir a utilização de regras para tratamento de eventos de logs e pacotes, geração de alertas e identificação de ameaças cibernéticas de forma automática, além de permitir a criação e customização, via console, de novas regras de alertas.

A solução deve possuir um canal online via Internet do próprio fabricante, para download e atualização de regras de correlação, interpretadores de logs e modelos de relatórios.

Ser capaz de consultar, periodicamente, bases de conhecimento e inteligência de ameaças tanto em fontes abertas quanto fechadas, de forma a alimentar seus mecanismos, baseado em múltiplos eventos e logs, com identificação de potenciais problemas ou comportamentos anômalos.

Deve permitir integração com fontes externas para enriquecimentos de eventos.

Permitir o processamento de informações estruturadas de ameaças Structured Threat Information eXpression e Trusted Automated eXchange of Indicator Information (STIX/TAXII), informando detalhes do indicador encontrado.

Deve possuir integração com fontes de inteligência aberta (OSINT - Open source intelligence) para detecção, em tempo real, de ameaças, incluindo, endereços IP, endereços de e-mail, URLs, hostnames e hashes de arquivos.

Implementar análise automática do tráfego de rede, fornecendo características sobre as sessões, quantidade de bytes transferidos e recebidos, sentido do fluxo, taxa de transferência e duração de sessão.

Implementar análise de tráfego de rede com capacidade de detecção de ameaças, incluindo atividades de beaconing, remote access Trojan (RAT), comando e controle (C2).

Implementar análise de logs para detecção de movimentação lateral de arquivos.

Implementar análise de tráfego de rede com capacidade de analisar características do protocolo HTTP e o conteúdo, incluindo o método HTTP, recurso, query, URL, formulários via POST, e identificação de ameaças, incluindo cabeçalhos não suportados, análise de cabeçalhos, análise de transações GET e POST, arquivos, hidden frames e embedded objects.

Suportar a utilização de regras baseados em Snort.

Ser capaz de identificar a troca de extensão de arquivos como, por exemplo, um arquivo executável (.exe) utilizando uma extensão .jpg.

Implementar o enriquecimento, em tempo real, utilizando dados como informações de ativos, nível de risco, inteligência de ameaças, tipo de evento, fonte de eventos, dispositivo, identidade, e outros elementos de dados.

Implementar integração com diretório Microsoft Active Directory para coleta de informações de usuários.

Implementar whitelist e blacklist para endereços IP, usuários, hosts para serem utilizados na geração de alertas.

Possuir mecanismos computacionais capazes de identificar potenciais problemas ou comportamentos anômalos, baseado em múltiplos eventos e logs, gerando alertas tanto no console centralizada e por e-mail.

Permitir detecção de padrões de sentido de conexões inbound (rede interna para Internet), outbound (Internet para rede interna) e lateral (rede interna para rede interna).

Permitir a identificação de nomes de redes definidos pelo administrador.

Permitir detecção de movimentos laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux.

Implementar regras de comportamento suspeito de usuários, devendo ser capaz de detectar, pelo menos, as seguintes anomalias:

- Conta adicionada e removida do grupo de administradores;
- Conta criada e excluída em seguida, dentro de um intervalo de tempo definido;
- Conta adicionada ao grupo de administradores pelo mesmo usuário que executou o comando;
- Registro de login de conta monitorada em uma watchlist;
- Falhas de logins sucedidas por um login bem-sucedido a alteração de senha;
- Falhas de logins sucedidas por um login bem-sucedido, acompanhado por alteração de senha;
- Falhas de logins fora do horário comercial;
- Falhas de logins de diferentes origens para o mesmo destino;
- Falhas de logins de diferentes usuários para o mesmo destino;
- Falhas de logins de um mesmo usuário de diferentes países;
- Falhas de logins de uma mesma origem com diferentes usuários;
- Logins bem-sucedidos de diferentes origens para diferentes destinos;
- Logins bem-sucedidos de diferentes origens para o mesmo destino;
- Múltiplos bloqueios de conta do mesmo usuário e de usuários diferentes;
- Falhas de escalonamento de privilégios de um mesmo usuário;
- Falhas de logins em um Domain Controller de um usuário administrador;
- Limpeza em massa de logs de auditoria;
- Limpeza dos logs de auditoria, firewall e compartilhamento do Windows;
- Suspeitas de movimentação lateral;
- Logins através de vários servidores.

Suportar integração com tecnologia de análise comportamental de usuários e entidades (UEBA utilizando as informações de eventos, logs e tráfego de rede, para a monitoração de segurança, gerando índices de riscos, alertas e incidentes para eventos de usuários e entidades mapeadas na mesma console de tratamento de eventos, alertas e incidentes da solução entregue.

Suportar integração com solução de detecção e resposta a incidentes em estações de trabalho e servidores, alertas e incidentes, com respectiva visibilidade, como também de processos, executáveis e bibliotecas, associação de processos com tráfego de rede, com o intuito de complementar a visibilidade entregue e capacidade de análise de atividade maliciosa.

Implementar relação de eventos com framework MITRE ATT&CK, devendo ser capaz de relacionar regras e alertas às táticas (Tactics) e às técnicas (Techniques) do framework.

Implementar, a partir de eventos e pacotes coletados, a identificação de IoC (Indicators of Compromise), padrões de tráfego e eventos que indicam comportamento de algo comprometido, assim como eventos e tráfegos que indique ações que aumentem a exposição a ameaças.

A solução deve alertar em tempo real sobre tráfego coincidente com assinaturas pré-definidas e permitir a visualização da sessão em que a assinatura ocorreu, assim como a exportação da sessão dados brutos.

O fabricante da solução deve disponibilizar informações de inteligência de ameaça integrada à solução para enriquecimento de eventos.

Permitir integração com outras soluções de segurança, por meio de alertas sobre qualquer dado ou comportamento definido em regras, e permitir o envio de alertas via protocolos SYSLOG e e-mail para plataformas externas, como SIEM ou servidor de syslog.

Deve permitir a criação de modelos de mensagens de e-mail para alertas, com textos definidos pelo administrador, e variáveis que serão substituídas por atributos do alerta.

Permitir, como ação de uma regra, a execução de scripts escritos em Ruby, Python e Bash Shell.

Deve permitir a criação de modelos de scripts de alertas, com acesso aos atributos do alerta para utilização pelo script.

Possuir mecanismo de exportação de eventos da solução para outras plataformas, incluindo compatibilidade com, pelo menos, Redis e Elasticsearch.

Possuir a funcionalidade para resolução de endereços IP, como localização da cidade, país e organização das conexões.

Permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados.

Permitir buscas com expressões em texto livre, que pode estar presente em qualquer metadado. Por exemplo, realizar uma busca por “arquivo.doc” e retornar eventos que possuam este valor em qualquer campo, e não apenas no “nome do arquivo”.

Permitir realizar buscas utilizando atributos do framework MITRE ATT&CK, utilizando valores mapeados nos eventos e alertas.

Permitir criação manual de incidentes a partir de alertas com a definição de risco e prioridade.

Permitir atribuir determinados tipos de incidentes para analistas de segurança, de forma manual e automática.

Permitir a criação e acompanhamento de incidentes de segurança, de forma manual ou automática.

Permitir inserir análise forense de logs e tráfego de rede como um complemento da análise do incidente.

Permitir registrar os resultados de um incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.

Permitir que sejam gerados relatórios de auditoria da própria solução.

Possuir um módulo para construção de relatórios customizados pelo analista, com funcionalidade do tipo arrastar-e-colar para definição dos campos e elementos.

Permitir que o analista possa filtrar logs e eventos ao gerar relatórios.

Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal, e sob demanda.

Permitir o agendamento de geração automática e manual de relatórios, com a possibilidade de envio por e-mail.

Possuir relatórios de conformidade e regulamentações pré-definidos como BASEL II, FERPA, FFIEC, FISMA, GLBA, ISO27002, NERC-CIP e NISPOM.

Possuir um relatório ou painel que demonstre o consumo de licenças em tempo real e histórico, o volume licenciado, a quantidade excedida, e a tendência de utilização.

3.2.8.2. Detecção e resposta em *endpoints*

A solução de Endpoint Detection e Response deverá ser fornecida, operada, suportada e customizada pela CONTRATADA, mediante edição de Ordem de Serviço específica.

Deve ser implantada por meio de módulo agente a ser instalado nos endpoints.

O módulo deve possibilitar uma administração via console de gerenciamento centralizado de todos os agentes. A console deve também ser acessível através de HTTPS e compatível com ao menos um dos navegadores de mercado (MS-Edge, Google Chrome, Mozilla Firefox).

A solução (console administrativo e agente) deverá dar visibilidade centralizada das ameaças, permitindo diagnóstico e remediação também de forma centralizada.

O agente deve suportar, pelo menos, os sistemas operacionais previstos no **Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**, bem como respectivas atualizações.

A comunicação do agente com o servidor de administração deve ser em túnel de segurança TLS criptografado.

A solução deve permitir a comunicação de agentes com a console central, mesmo se estiverem fora da rede interna da Contratante, possibilitando a correta atualização periódica dos componentes da solução.

A instalação deve ser feita através de solução de Deployment remoto fornecida pela Contratada. Em dispositivos Windows pertencentes a domínio Active Directory, a solução também deve permitir instalação dos agentes através de GPO.

A solução deve possibilitar a execução remota de scripts Powershell(máquinas Windows) ou Bash Script (máquinas Linux) em caso de tratamento de incidente.

A gerência de administração deve ser capaz de arranjar os endpoints gerenciados através de grupos via seleção manual ou através de regras de agrupamento automatizadas com base em no mínimo, os critérios abaixo:

- Domínio
- Endereço IP
- Endereço de rede (CIDR)

- Hostname parcial ou completo
- Sistema Operacional
- Versão do agente
- Unidade Organizacional do Active Directory

Detectada mudança em determinada informação que enseje mudança de grupo, o sistema deve ser capaz de atualizar de forma automática o novo grupo do endpoint.

A solução deve permitir a aplicação de políticas de detecção e resposta para grupos de endpoints ou para endpoints individuais.

Deve ser possível a definição de perfis com acessos limitados para usuários dentro da gerência de administração da solução, delimitando as permissões e/ou acesso as funcionalidades. A solução deve permitir integração com grupos do Active Directory.

Deve possuir proteção de desinstalação através de senha ou token em cada endpoint gerenciado.

Deve ter mecanismos que garantam que seu funcionamento não possa ser interrompido por usuários sem perfil com privilégios administrativos.

Deve detectar e logar tentativas de manipulação indevida dos seus componentes.

Deve possibilitar, através de políticas, o controle de acesso (bloqueio/liberação de leitura,escrita e gravação) de dispositivos diversos como HD (hard disks) externos, pendrives USB, storages removíveis, CD, DVD, interfaces de rede sem fio, modems, bluetooth, infravermelho, além de MTP (Media Transfer Protocol), tais como iPhone e o Android smartphone.

Deve possuir funcionalidades de Firewall/IPS, e possibilitar:

- Atualização periódica de novas assinaturas de ataque;
- Criação de regras centralizadas em políticas para definir com precisão o tráfego permitido para entrada e saída do endpoint. Tais regras podem estar ativas ou inativas;
- Possibilitar o suporte minimamente dos protocolos Any, TCP, UDP, ICMP e avançado (especificado pelo usuário), da especificação de endereço local, porta local, endereço remoto, porta remota, podendo configurar para cada conexão permissão, bloqueio, sentido do fluxo (Inbound/Outbound/Inbound e Outbound). A configuração do endereçamento deve permitir o cadastro de listas específicas de IPs ou range de IPs (IPv4 e Ipv6);
- Reconhecimento e bloqueio automático de aplicações em clientes, baseando-se no hash do arquivo;
- Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
- Um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

A solução deve prover auditoria detalhada com, no mínimo, as seguintes ações administrativas:

- Criação/Deleção de grupos
- Adição de exclusões
- Autenticação de usuário
- Criação/Alteração/Deleção de políticas
- Início de isolamento de rede
- Manutenção de permissões de perfis/usuários.

Quanto aos relatórios, a solução deverá prover dashboard trazendo as detecções mais recentes.

A solução deve contemplar, no mínimo, as seguintes visualizações:

- Agentes ativos;
- Agentes por sistema operacional;
- Detecções por severidade do ataque;
- Reporte de detecções, ao menos agrupados pelas seguintes opções:
    - Por máquina;
    - Por severidade;
    - Deve ser possível filtrar por:
        - Severidade;
        - Host;
        - Sistema operacional;
        - Versão do Sistema Operacional;
        - Opções de períodos (ex: última hora, última semana, etc) ou período personalizado;
        - Nome de arquivo;
        - Hash de processo.

Deve gerar relatório dos endpoints monitorados contendo minimamente as seguintes informações:

- Hostname;
- Data e hora da última comunicação;
- Versão do sistema operacional;
- Unidade organizacional (OU);
- Política de proteção aplicada;
- Política de resposta aplicada;
- Política de atualização aplicada;
- Política de firewall aplicada;
- Identificação do host (UID/GUID);
- IP local da máquina;
- Subnet da máquina;
- IP público da máquina;
- MAC Address;
- Versão do sensor/agente instalado;
- Versão da base de conhecimento/assinatura/referência;
- Data da última verificação;
- Situação (ver próximo item).

A solução deve gerar relatório quanto a situação dos endpoints, tendo ao menos as seguintes classificações (podendo ter mais de uma situação):

- Sem ameaça detectada;
- Com ameaça detectada;
- Sem comunicação há muito tempo/Sem gerenciamento;
- Bloqueado/isolado;
- Versão da base de conhecimento/assinatura/referência;
- Verificação completa não realizada há muito tempo;

- Endpoint com EDR inativo;
- Endpoint sem EDR.

Quanto à capacidade de investigação, detecção e resposta de ameaças, a solução deverá:

- Ser capaz de detectar e bloquear em tempo real ameaças conhecidas (ex Keyloggers, Trojans, Worms, Rootkits, Botnets, Spywares, Adwares, etc) e desconhecidas (zero-day), ataques fileless, ameaças avançadas (APTs), Ransomwares, exploits e outros comportamentos maliciosos;
- Possibilitar configurar listas de exclusão (Whitelist) de arquivos, diretórios, aplicações e recursos Web para que não sejam verificados pelo produto;
- Permitir a varredura das ameaças a partir da console de gerenciamento, de maneira manual, agendada e em tempo real na máquina do usuário. A varredura deverá poder ser feita em background, sem comprometer a performance das atividades do usuário;
- Realizar a atualização das vacinas várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
- Manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
- Proteger a navegação na web, para todos os principais navegadores (IE, Firefox e Chrome) e possibilitar a configuração de lista negra de URLs/domínios proibidos. Bloquear a navegação também pela verificação dos dados baixados antes de serem executados;
- Permitir que administradores possam interromper ou bloquear tráfego de rede de endpoints classificados como comprometidos. O tráfego deve ser restrito somente com a gerência de administração da solução para efetuar análise e diagnóstico aprofundado, e posteriormente readmitir o endpoint quando ele estiver saneado;
- Dispor de um módulo de configuração de alertas em caso de detecção de eventos críticos e disponibilizados em um Dashboard para acompanhamento. Possibilitar notificação imediato do cliente via gerência de administração da solução, notificando também através de envio e-mail;
- Fornecer, para as detecções, análise completa, com notas explicativas e recomendações para remediação;
- Ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;
- Ser capaz de exibir todos os processos, acessos, arquivos e chaves de registros gerados pela ameaça;
- Ser capaz de exibir linha de comando gerada pelo processo suspeito;
- Permitir visualizar toda a cadeia de ataque, permitindo assim análise de causa raiz;
- Ser capaz de coletar e enviar à console de administração dados sobre a telemetria das ações realizadas nos endpoints, no mínimo, das seguintes atividades:
    - Informações de rede como endereço IP de origem e destino, portas de origem e destino;
    - Login de usuários;
    - Versão, grupo de usuários locais, membros de grupos de usuários locais, e usuários locais;
    - Número de executáveis únicos;
    - Processos que foram criados, finalizados, hash, PID, User Time, comando que iniciou o processo e Threads criados pelo processo;
    - Utilização de ferramentas administrativas;

- Requisições DNS;
- Conexões de rede incluindo portas e processos associados;
- Informações sobre nome do arquivo, data de leitura, data de criação, data de modificação, e data de exclusão;
- Arquivos compactados escritos;
- Scripts escritos em disco;
- Scripts executados;
- Informações sobre registros de sistema: data de criação, data de leitura, data de modificação, e data de exclusão. Os valores deverão constar nos registros;
- A consulta à trilha de auditoria/telemetria deve ser possível de ser feita via console de gerenciamento centralizada.

- Permitir extração de indicadores de comprometimento (IOC) como hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de e-mail, nomes de arquivos associados às atividades maliciosas;
- Ser capaz de detectar ameaças mesmo não estando conectado à internet;
- Ser capaz de classificar, quando aplicável, as detecções de acordo com os códigos das técnicas e táticas do MITRE ATT&CK
- Bloquear scripts e comandos em Powershell considerados suspeitos;
- Efetuar bloqueio automático de processos suspeitos;
- Efetuar bloqueios baseado em centros de inteligências do fabricante quanto a reputação de arquivos, recursos da Web e softwares;
- Efetuar bloqueio de operações suspeitas no registro do Windows;
- Ser capaz de proteger contra ataques que exploram corrupção de memória;
- Possibilitar, via console central, o bloqueio remoto de comandos suspeitos executados remotamente que tenham como finalidade:
  - extração de arquivos
  - envio de arquivos para um repositório externo
  - início de um processo
- Ser capaz de proteger processos do sistema em memória;
- Em caso de Ramsonware:
  - Dispor de capacidade de proteção não baseada exclusivamente em assinaturas;
  - Ser capaz de detectar malwares do tipo Ransomware ao menos com base nas ações a seguir:
    - Deleção de backups
    - Operações em excesso ao sistema de arquivos
    - Criptografia de arquivos
      Processos associados a malwares de Ransomware
  - Prevenir ameaças e interromper que elas sejam executadas em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas;
  - No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal realizando a limpeza e remoção completa do ransomware na máquina do usuário;
  - Numa eventual detecção, fornecer uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas

as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados;

- Ser capaz de detectar e bloquear exploração baseado em, no mínimo, os seguintes comportamentos:
    - Criação de processos suspeitos originados de navegadores;
    - Detecção de comprometimento de servidores Web através de webshell;
    - Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução;
    - Injeção de código não esperada de um processo a outro;
    - Execução de Java Script através do executável Rundll32;
- Ser capaz de detectar e bloquear movimento lateral quando burla o processo de logon do Windows;
- Ser capaz de detectar e bloquear processos que tentam obter credenciais de login;
- Deletar os arquivos maliciosos ou movê-los para área de quarentena de acordo com a política estabelecida;

Deve suportar investigação de ações maliciosas nos padrões YARA e OpenIOC ou superiores.

Deve permitir a escolha dos alvos de investigação através de Estação de trabalho registradas na console, com os seguintes filtros: nome da estação, endereço IP, nome de usuário, nome do arquivo, hash, chave de registro, linha de comando e OpenIOC.

Deverá registrar e armazenar as informações sobre os comportamentos do sistema, comunicações e comportamentos do usuário, que estejam no escopo do endpoint protection.

A investigação deve permitir o isolamento utilizando Windows Filtering Platform (WFP).

O resultado da investigação deve conter informações sobre a máquina alvo, endereço IP, último usuário logado, primeira vez que o objeto foi visto na rede, nome do objeto, e identificação se o objeto é suspeito ou malicioso.

O Módulo de Investigação deverá permitir finalizar o processo malicioso na cadeia de investigação de EDR.

Deverá permitir a visualização e diagnóstico de eventos de segurança com base no histórico dos eventos registrados.

Deve permitir a criação de gatilhos para eventos específicos que executará script em PowerShell; VB; e BAT ou outras ações customizáveis.

O servidor de gerenciamento deve ser compatível o ambiente tecnológico da CONTRATANTE (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**).

Quanto ao gerenciamento de vulnerabilidades, a solução deverá:

- A solução deverá identificar vulnerabilidades em hosts Windows e Linux, incluindo vulnerabilidades do sistema operacional e de aplicações comuns.
- Identificar de acordo com frameworks da indústria tais como:
    - NIST's National Vulnerability Database (NVD);
    - Mitre's Common Vulnerabilities and Exposures (CVE);
    - Common Vulnerability Scoring System (CVSS) score;
- Mostrar patches já instalados no host;

- Monitorar continuamente e detectar quando um update ou uma aplicação foi instalado;

Quanto ao inventário de dispositivos, usuários e aplicações, a solução deverá:

- Para os dispositivos:
  - Possibilitar a visualização de ativos que foram adicionados ou removidos;
  - Possibilitar a detecção do de novos ativos na rede;
  - Informar se há criptografia de disco;
- Para os usuários:
  - Deverá permitir o acompanhamento das alterações de senha;
  - Monitorar o uso das credenciais (inclusive os que já vem com a OS, bem como os locais) e os ativos acessados;
  - Monitorar atividades de login bem-sucedida e com falha;
- Para as aplicações:
  - Rastrear aplicações instaladas nas máquinas;
  - possibilitar a não inicialização/bloqueio personalizado de aplicações através de inclusão de assinaturas digitais (hashes) de arquivos;

Quanto à capacidade de emulação de execução de código, a solução deverá:

- Prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, podendo ser em nuvem do fabricante;
- Se integrar ao agente instalado em endpoints para permitir que arquivos suspeitos sejam enviados ao serviço de emulação de execução;
- Emular execução, no mínimo, dos principais sistemas operacionais, em especial aqueles previstos no ambiente tecnológico da CONTRATANTE (**Item 9 Ambiente Tecnológico** da **Especificação detalhada do objeto (1.1.1)**).

3.3. Serviço de resposta aos incidentes de segurança/privacidade:

3.3.1. **Descrição**: integrante de um *Security Operations Center* (SOC) irá analisar, remediar, conter e documentar os eventos/incidentes de segurança da informação, como ainda, fornecer a devida orientação técnica à contratante e aos demais prestadores de serviços correlatos ao tema deste objeto contratual, na obtenção da solução para incidentes, bem como implementar respostas automatizadas a determinados eventos.

3.3.2. **Objetivo a ser atingido**: obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas, oferecer as respostas (preferencialmente automatizadas) aos incidentes de segurança da informação, nos quais se incluem eventos relacionados à quebra da privacidade de informações pessoais e sensíveis, com a conseguinte restauração do ativo/serviço/processo.

3.3.3. **Medição**: o serviço será fornecido de forma contínua, mensalmente e independe de qualquer métrica e deve obedecer ao o **Acordo de Nível de Serviços** (**Item 8** da **Especificação detalhada do objeto (1.1.1)**).

3.3.4. Processo de resposta aos incidentes de segurança/privacidade:

Incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da CONTRATANTE, que venha prejudicar um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade e Não-repúdio.

O início do processo de resposta a incidente de segurança se dará sempre que um evento adverso for submetido pelos demais serviços objetos deste contrato.

A qualquer tempo, a CONTRATANTE poderá abrir um incidente de segurança.

Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, analisar artefatos e apresentar um diagnóstico contendo todas as informações relevantes, tais como tipo de incidente, severidade, origem, ativos e/ou serviços comprometidos, riscos, linhas de ação a serem seguidas e aspectos temporais envolvidos, bem como informações acerca da atuação do atacante, de como como ocorreu o acesso, de quais ativos foram acessados e/ou danificados.

A severidade do incidente de segurança da informação será parametrizável e atribuída pela propria ferramenta, mas com a possibilidade de passar por reclassificação, a critério da CONTRATANTE.

Todo o processo de análise e resultados obtidos, devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que a CONTRATANTE acompanhe todos os passos até a solução definitiva do problema.

A CONTRATADA, deverá definir e executar uma estratégia para a mitigação e contenção do ataque.

Qualquer tipo de alteração no parque computacional da CONTRATADA deverá ser previamente autorizada pelo corpo técnico da CONTRATANTE que deverá, dentre quaisquer outros aspectos, considerar o plano de recuperação de desastres e a política de segurança da informação.

Mitigado o incidente de segurança, a CONTRATADA, com auxílio do Blue Team, iniciará o processo de recolhimento de todas e quaisquer evidências e identificação dos serviços e ativos afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

Em seguida, deve-se ativar o processo de restauração dos ativos e serviços afetados, em comum esforço com a CONTRATADA e respectivos times próprios/terceirizados, naquilo que compete a cada parte envolvida.

Por fim, deve-se realizar análise forense do ocorrido e providenciar documentação conclusiva, que servirá de ponto de partida para adequações nos ativos, serviços sistemas e/o processos.

Caso seja necessária a reconstrução do ataque, este deve ser realizado pela CONTRATADA em ambiente controlado, usando-se por exemplo de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da CONTRATADA.

3.3.5. Interface com demais serviços: sempre que possível, as interfaces entre serviços devem operar de forma integrada, de forma atingir os respectivos objetivos descritos.

3.3.6. Entregáveis:

A CONTRATADA deve entregar:

3.3.6.1. Inicialmente, relatório com plano de ação para os principais (e quais) ataques que possam a vir comprometer o ambiente.

3.3.6.2. Quando for o caso, relatório em formatos (PDF, CSV e HTML) contendo informações acerca dos eventos ocorridos.

3.3.6.3. Mensalmente, quantitativo de incidentes registrados com, em sendo o caso, as seguintes informações correlatas:

- Data do incidente
- Id no sistema de monitoramento
- Tipo de Vulnerabilidade
- Tipo de Ataque
- País de Origem
- IPs
- Tipo de Evento
- Regra de Correlacionamento
- Severidade
- Área Responsável
- Ativo alvo específico
- Categoria do Alvo: Aplicação Web; Dispositivo; Container
- Demais atributos que a CONTRATANTE/CONTRATADA possam sugerir.

3.3.7. Referência ao SLA: ver o **Acordo de Nível de Serviços** (**Item 8** da **Especificação detalhada do objeto (1.1.1)**)

3.3.8. Especificações técnicas:

Para execução deste serviço, a CONTRATADA deverá fornecer, utilizar e ser capaz de operar, sustentar e suportar ferramenta de gestão de operações de segurança, com características descritas nos pontos abaixo.

3.3.8.1. Incidentes de Segurança

Em sendo o caso, o sistema de correlação de eventos (SIEM), fornecido pela CONTRATADA, deverá fornecer integração para recebimento de alertas e abertura automática de incidentes, para tratamento via fluxo de trabalho. A plataforma contratada deverá suportar o recebimento de alertas em formato Syslog.

Permitir o acesso a distintos painéis de controle, totalmente customizáveis sem a necessidade do uso de programação, através da utilização de perfis diferenciados. Dentre os perfis disponíveis, a plataforma deverá, no mínimo, contemplar os seguintes dashboards/perfis específicos:

- Analista Nível 1. Responsável pela triagem inicial dos eventos;
- Analista Nível 2. Responsável pela análise mais detalhada dos eventos;
- Coordenador do SOC. Coordenador da equipe de analistas;
- Gerente do SOC. Gestor responsável por todo o SOC;

- Coordenador de Brechas de Segurança. Responsável pelo acompanhamento das Brechas de Segurança que ocorreram no ambiente, junto a profissional indicado pela CONTRATANTE;
- Analistas de TI. Responsáveis pelo tratamento de tickets que envolvam ativos de TI.

Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática com, no mínimo, as seguintes características:

- Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente (SIEM). Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;
- Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes, e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
- Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc.

Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e fonte (SIEM).

Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente.

Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise.

Permitir inserir análise forense de host e rede, como um complemento da análise do incidente.

Inserir análise de impacto relativo à Confidencialidade, Integridade e Disponibilidade, incluindo informações existentes sobre Brecha de Segurança tais como: data, status, dispositivos envolvidos e descrição.

Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.

Permitir o recebimento de Alertas de Segurança com as seguintes características:

- Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;
- Dados de origem e destino, portas de origem e destino, domínios de origem e destino, endereço MAC de origem e destino, além de informações de contexto de negócios de cada dispositivo (de origem ou destino). As informações de contexto deverão incluir endereço IP, nome do dispositivo, tipo, unidade de negócios, site, índice de criticidade e conformidade, além do proprietário, tanto para os dispositivos de origem quanto dispositivos de destino. É necessário também, incluir informações de localização do dispositivo, incluindo cidade, país e

geolocalização, tanto dos dispositivos de origem quanto dos dispositivos de destino dos alertas.

Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas.

Permitir a criação de Investigações de Incidentes que não sejam necessariamente relacionados à Segurança da Informação, que permitam o atendimento às seguintes características: data de criação, status, prioridade, dias em aberto, tipo de investigação (exemplo: hacking, má conduta, violação de ética, etc), identificação de confidencialidade, datas de início e término da investigação, título, sumário, analista atribuído, nome do solicitante, fonte, tipo de requisição, nível de urgência.

3.3.8.2. Brechas de Segurança

Possibilitar a documentação de Brechas de Segurança com as seguintes características:

- Status, data de criação, dias em aberto, usuário que identificou a brecha, método de descoberta, tipo, data da ocorrência, data de descobrimento, datas de início e fechamento da resposta, nome da brecha e descrição detalhada;
- Descrição das informações vazadas, incluindo o tipo, número total de registros, informações sobre encriptação, vetor de transferência (vazamento) e tipo de dado (eletrônico, etc), além da identificação dos vazamentos por regiões.

Possibilidade de inclusão de comentários de atividades por parte dos analistas, permitindo desta forma a identificação clara de todo o processo investigativo.

Definição de tarefas a serem executadas durante uma Brecha de Segurança.

Definição de notificações a serem enviadas para os envolvidos em uma investigação de Brecha de Segurança. Estas notificações deverão incluir informações como, o contato a ser acionado primeiro e os contatos sequenciais. Também deverá ser possível definir a mensagem a ser enviada na notificação.

Possuir uma base de dados de procedimentos de Resposta a Brechas.

Permitir a definição de Controles de Segurança.

Permitir atrelar os Controles de Segurança a Incidentes efetivos e inefetivos permitindo assim a medição de sua efetividade.

Possibilitar a criação de Políticas de SOC com a definição de proprietário e descrição dos detalhes, além da definição das partes interessadas.

Permitir a definição de contatos que inclua detalhes de endereço, telefones, localização, bem como informações sobre conhecimentos técnicos, formação, etc.

Permitir a definição de times de analistas.

Enviar um lembrete e notificações de escalonamento conforme a data final de uma avaliação que se aproxima.

3.4. Serviço de inteligência aplicado à segurança da informação:

3.4.1. **Descrição**: fazer buscas contínuas em Deep e Dark web sobre a CONTRATANTE e pessoas por ela definidas, em busca de informações acerca dessas pessoas, links falsos, documentos falsos, urls parecidas com as oficiais, que possam induzir fraudes, como principalmente a retirada "takedown" (independente da localidade em que se situa) dos respectivos endereços, endpoints, links, domínios e congêneres junto às empresas e aos órgãos competentes

3.4.2. **Objetivo a ser atingido**: buscar, de forma eficaz e proativa, dados ilegítimos, fraudes e/ou vazamentos de dados e credenciais que envolvam a CONTRANTANTE em suas funções institucionais e pessoas que integrem seu respectivo quadro de profissionais.

3.4.3. **Medição**: o serviço será fornecido de forma mensal, contínua e independe de qualquer métrica.

3.4.4. Processo de identificação: a CONTRATADA deverá apresentar proposta de uso de ferramentas, regras, análises e mecanismos pelos quais pretende atuar para atingir o objetivo descrito no **Item 3.4.2 supra**.

Em seguida a CONTRATANTE emitirá Ordem de Serviço, homologando a proposta de atuação da CONTRATADA e, por conseguinte, dando autorização para início do serviço.

3.4.5. **Interface com demais serviços**: sempre que possível, as interfaces entre serviços devem operar de forma integrada, de forma atingir os respectivos objetivos descritos.

3.4.6. **Entregáveis**:

A CONTRATADA deve entregar mensalmente ou quando solicitada:

3.4.6.1. Diagrama didático e atualizado da estrutura, ferramentas e regras utilizadas.

3.4.6.2. Relatório em formatos (PDF, CSV e HTML) contendo informações acerca dos eventos registrados, de forma que seja possível a realização de análises mediante aplicação de filtros, geração de gráficos e/ou cruzamentos de informações possam ser efetuados.

3.4.7. **Referência ao SLA:** ver o **Acordo de Nível de Serviços** (**Item 8** da **Especificação detalhada do objeto (1.1.1)**)

3.4.8. **Especificações técnicas**:

As especificações técnicas são como balizas para a definição de requisitos do serviço, mas que devem ser interpretadas sempre de forma a possibilitar o alcance do objetivo definido (**Item 3.4.2 supra**).

O serviço de inteligência aplicada a segurança, deve:

Não limitar quantidade de recursos pesquisados.

Prover pesquisa direcionada através da monitoração de palavras pré-selecionadas fornecidas.

Permitir a pesquisa de informações nos seguintes contextos:

- Ameaças cibernéticas;
- Resposta a Incidentes;
- Proteção da denominação institucional da CONTRATANTE;
- E-mails e domínios definidos pela CONTRATANTE.

Realizar descoberta de páginas web de “phishing”, ativas utilizando o nome dos recursos pesquisados, a marca, identidade visual, domínios e ativos que serão protegidas.

Realizar validação de sites suspeitos em repositórios sob demanda de “phishing” com validação das entidades reguladoras como ICANN (Internet Corporation for Assigned Names and Numbers) e Registro.Br (Registro de Domínios para a Internet do Brasil).

Realizar a detecção de domínios recentemente registrados que possam oferecer riscos e serem utilizados de forma maliciosa, por exemplo:

- Variações comuns de nomes;
- Permutações de caracteres;
- Desvio de URL (typosquatting).

Suportar a extração de informações considerando, no mínimo, as redes conhecidas como Clear Web (Internet aberta), Deep Web (Internet profunda) e também a Dark Web (Internet negra).

Informar anomalias nos registros “WhoIS” dos domínios monitorados.

Identificar as vulnerabilidades dos domínios monitorados que foram tornadas públicas.

Alertar a respeito de novas vulnerabilidades que tenham sido recentemente divulgadas em ambientes Linux (CentOS, RedHat e CentOS Stream) e Windows Server a partir de 2003.

Alertar a identificação de possíveis intenções de ataques a vulnerabilidades conhecidas que afetem os ambientes protegidos.

Alertar para intenções de ataque que tenham como objetivo os recursos pesquisados ou o seu nicho de atuação.

Alertar sobre campanhas relevantes de “hacktivismo”.

Alertar sobre atividades fraudulentas relacionadas aos recursos pesquisados (utilização indevida de nome e marca, por exemplo).

Identificar credenciais de acesso que estejam a venda em mercados negros online.

Alertar a respeito de códigos maliciosos (malwares) direcionados para os recursos pesquisados.

Indicar ações ativistas contra os recursos pesquisados.

Identificar intenções diretas de ataques aos recursos monitorados.

Alertar sobre discussões online que divulguem ou acompanhem informações dos recursos monitorados.

Identificar sobre perfis falsos que utilizem os nomes e/ou fotos das pessoas monitoradas.

Identificar vazamentos de credenciais e dados pessoais das pessoas monitoradas.

Detectar documentos ou informações confidenciais vazadas dos recursos monitorados.

Identificar aplicativos maliciosos que utilizem o nome, a marca ou identidade visual dos recursos pesquisados.

Identificar desfiguração de páginas (defacement).

O sistema do serviço de inteligência aplicada a segurança, deve permitir:

- O envio de alertas via e-mail dos eventos coletados e enviados para a plataforma;
- A emissão de relatórios e gráficos;
- Que todos os relatórios e gráficos sejam exibidos no painel de bordo (dashboard) e exportar os resultados para os seguintes formatos: CSV ou planilha eletrônica;
- O serviço deve emitir relatórios de inteligência sobre ameaças iminentes e tendências em períodos de tempo pré-definidos, conforme listados abaixo:
    - Semanal;
    - Mensal;
    - Anual.

3.5. Serviço de testes de invasão:

3.5.1. Descrição: uso de técnicas e ferramentas especificas (estáticas ou dinâmicas) para tentar obter acesso não autorizado e privilegiado aos ativos e informações, definidos em Ordem de Serviço específica.

3.5.2. Objetivo a ser atingido: identificar, mapear, documentar, controlar e auxiliar na correção e, em sendo o caso, corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica e de segurança da informação.

3.5.3. Medição: o serviço será fornecido e medido por meio dos seguintes itens:

3.5.3.1. Hora-Homem

3.5.4. Processo de testes de invasão:

O serviço de Testes de Invasão deve seguir o rito de Atividades Projetizadas descrito no **Item 6 - Modelo de Faturamento** da **Especificação detalhada do objeto (1.1.1)**.

A CONTRATANTE deverá apresentar o ambiente sistemas e demais ativos envolvidos que deseja ser alvo de testes, em ambiente próprio ou de terceiros.

A CONTRATADA deverá apresentar ferramentas, técnicas e metodologias que julgar pertinente para o escopo apresentado, bem como um cronograma, quantidade de horas que pretende alocar para o escopo apresentado, bem como quais os resultados esperados.

Os alvos dos “Testes de Invasão” bem como as premissas e condições para realização dos mesmos serão, necessariamente, definidos e aprovados através de Ordem de Serviço (OS) específica.

A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa da CONTRATANTE) ou externamente (através da Internet).

Todas as fases dos "Testes de Invasão" serão acompanhadas e supervisionadas a critério do CONTRATANTE.

Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo, deverá ser imediatamente reportada - antes de sua execução - haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

Além do rito de Atividade Projetizada, o teste de invasão e respectiva Ordem de Serviço deverá englobar\obedecer às seguintes fases:

- Planejamento;
- Descoberta;
- Ataque;
- Relatório Teste de Invasão;
- Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste, reavaliação, novo teste pós remediação.

3.5.5. Interface com demais serviços: sempre que possível, as interfaces entre serviços devem operar de forma integrada, de forma atingir os respectivos objetivos descritos.

3.5.6. Entregáveis: após execução de cada OS, deve-se fornecer o Relatório de Teste de Invasão.

3.5.7. Referência ao SLA: ver o **Acordo de Nível de Serviços** (**Item 8** da **Especificação detalhada do objeto (1.1.1)**).

3.5.8. Especificações técnicas:

As especificações técnicas são como balizas para a definição de requisitos do serviço, mas que devem ser interpretadas sempre de forma a possibilitar o alcance do objetivo definido (**Item 3.5.2 supra**).

A atividade de Testes de Invasão poderá ser do tipo Externo e/ou Interno, e terá como objetivo principal, identificar, mapear, documentar, controlar e sugerir correções para possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Estes testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações.

Farão parte do escopo dos testes de invasão:

- Aplicações web;
- Ativos de rede com IP;
- Containers de aplicações.

Para a realização dos testes de invasão, deverão servir de referência padrões internacionais, tais como:

- OSSTMM 3 (The Open Source Security Testing Methodology Manual);
- ISSAF/PTF (Information Systems Security Assessment Framework);
- NIST Special Publication 800115 (Technical Guide to Information Security Testing and Assessment);

- NIST Special Publication 80042 (Guideline on Network Security Testing);
- OWASP TESTING GUIDE 3.0 The Open Web Application Security Project.

Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos.

A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa da CONTRATANTE) ou externamente (através da Internet).

Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério do CONTRATANTE.

Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo, deverá ser imediatamente reportada - antes de sua execução - haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

O teste de invasão deverá obedecer às seguintes fases:

- Planejamento;
- Descoberta;
- Ataque;
- Relatório Teste de Invasão, inclusive com documentação das formas de reproducibilidade dos problemas apontados;
- Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste.

3.5.8.1. Planejamento

Todas as premissas, processos, atividades descritas e aprovadas na OS, inclusive os cronogramas, serão detalhadas e apresentadas na fase de planejamento.

Informações sobre o ambiente corporativo,.

Quais técnicas deverão ser usadas:

- Técnica da caixa preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista);
- Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste);
- Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo);
- Análise Estática.

3.5.8.2. Descoberta

Deverão ser utilizadas ferramentas de Análise de Vulnerabilidades, bem como técnicas manuais de análise de vulnerabilidade. As ferramentas deverão ser apresentadas para ciência e prévia aprovação, antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades, de forma a atingir ao objetivo acima (**Item 3.5.2** da **Especificação detalhada do objeto (1.1.1)**) descrito

Na fase da DESCOBERTA, deverão ser atendidos os seguintes quesitos, os quais deverão ser apresentados juntamente no “RELATÓRIO TESTE DE INVASÃO”:

Coleta passiva, na qual poderão ser exemplificativamente utilizadas as seguintes técnicas:

- Whois e nslookup (consultas DNS);
- Sites de busca;
- Listas de discussão;
- Blogs de colaboradores;
- Dumpster diving ou trashing;
- Informações livres;
- Packet sniffing “passive eavesdropping”;
- Captura de banner.

Coleta ativa, na qual poderão ser exemplificativamente utilizadas as seguintes técnicas:

- Port scanning (Mapeamento de rede);
- Varredura de vulnerabilidade.

A varredura de vulnerabilidade deverá verificar/identificar, entre outros:

- Hosts ativos na rede;
- Portas e serviços em execução;
- Serviços ativos e vulneráveis nos hosts;
- Sistemas operacionais;
- Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas; configurações feitas nos hosts sem observância de boas práticas em segurança computacional;
- Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;
- Identificação de vetores de ataque e cenários para exploração;
- Vulnerabilidades Detectadas (CVE);
- Vulnerabilidades de Alto Risco;
- Vulnerabilidades de Médio Risco;
- Vulnerabilidades de Baixo Risco;
- Informações a serem aplicadas na fase de ataques;

Acerca da análise de serviços e aplicações web, deve-se verificar:

- Uso indevido de sistema de arquivos e arquivos temporários;
- Evasão de informação por configurações default de tratamento de erros;
- Tratamento indevido de entrada;
- Problemas relacionados a má configuração dos serviços;
- Gerenciamento inseguro de sessões web.

3.5.8.3. Ataque/Exploração

Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada - antes de sua execução - haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

Deverá realizar testes de vulnerabilidades e invasão em endereços IP's, URL´s, aplicações, ou outro ativo definido do ambiente computacional, composto por servidores, banco de dados, ativos de rede, ativos de segurança, e outros equipamentos relacionados ao teste de invasão.

Será possível, para esse serviço, incrementos de Ordem de Serviço, de forma a planejar continuidade de testes em pontos específicos, descobertos nas fases iniciais.

Deverão ser aplicados exemplificativamente os seguintes tipos de ataques:

- Violações do protocolo HTTP;
- SQL Injection;
- LDAP Injection;
- Cookie Tampering;
- CrossSite Scripting (XSS);
- Directory Transversal;
- Buffer Overflow;
- OS Command Execution;
- Command Injection;
- Remote Code Inclusion;
- Server Side Includes (SSI) Injection;
- File disclosure;
- Information Leak;
- Zero day attacks;
- DDos (Distribuited Denial of Service);
- Dos (Denial of Service);
- Contra protocolo TCP;
- Ataques contra a aplicação.

Os ataques de negação de serviços contra protocolo TCP e em nível da aplicação, deverão, cada qual, explorar/demonstrar/utilizar, pelo menos, as seguintes técnicas:

- Bugs em serviços, aplicativos e sistemas operacionais;
- SYN flooding;
- Fragmentação de pacotes de IP;
- Smurf e fraggle;
- Teardrop, nuke e land;
- Para ataques contra o protocolo TCP:
    - Sequestro de conexões;
    - Prognóstico de número de sequência do protocolo TCP.
- Ataque de Mitnick / Source routing;
- Para ataques em nível da aplicação:
    - Buffer Overflow;

  - Problemas com o SNMP;
  - Vírus, worms e cavalos de Tróia.
- Injeção de Código:
  - Ataques XSS (Crosssite Script); Comprometimento do acesso remoto;
  - Manutenção de acesso.
- Encobrimento de rastros da invasão.

Para testes de invasão direcionados, especificamente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados testes baseados na publicação OWASP TESTING GUIDE 4.2 ou mais atual.

O resultado de cada teste deverá vir acompanhado de relatórios, contendo:

- Referência base (Whitepaper);
- Ameaças encontradas;
- Riscos levantados ao ambiente computacional;
- Formas e instruções para reproducibilidade das falhas
- Contramedidas para mitigar as ameaças encontradas.

3.5.8.4. Relatório de Teste de Invasão

Após a fase de ataque, deverá ser elaborado e entregue, o relatório "RELATÓRIO TESTE DE INVASÃO" para cada teste que será realizado, contemplando, no mínimo, as seguintes informações:

Objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas, instruções para reprodução do teste realizado e demais evidências do sucesso da invasão.

Será realizada reunião, conduzida pela CONTRATADA, para apresentação de forma detalhada de todo o conteúdo do "Relatório Teste de Invasão", onde serão sanadas todas as dúvidas do corpo técnico do CONTRATANTE.

3.6. Serviços técnicos especializados:

3.6.1. Descrição: serviços técnicos especializados e projetizados, para necessidades correlatas, novas implementações e/ou suporte de soluções de segurança da informação, durante o período de execução do contrato, desde que não conflitam ou pertençam ao objeto já estabelecido no presente termo de referência.

3.6.2. Objetivo a ser atingido: suprir necessidade correlata ou derivada, de temática associada à execução contratual.

3.6.3. Medição: o serviço será fornecido e medido por meio dos seguintes itens:

3.6.3.1. Hora – Homem

3.6.4. Processo de atividades projetizadas: ver itens 6 – Modelo de Faturamento, 8 – Acordo de Nível de Serviço da **Especificação detalhada do objeto (1.1.1) e 6.5. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS do respectivo Termo de Referência.**

3.6.5. Referência ao SLA: ver o **Acordo de Nível de Serviços** (**Item 8** da **Especificação detalhada do objeto (1.1.1)**)

3.6.6. Especificações técnicas:

As especificações técnicas são como balizas para a definição de requisitos do serviço, mas que devem ser interpretadas sempre de forma a possibilitar o alcance do objetivo definido (**Item 3.6.2**).

Os Serviços Gerenciados de Segurança devem englobar a prestação de serviços técnicos evolutivos em segurança da informação, sob demanda.

Os serviços devem ser baseados em horas de serviço, envolvendo atividades a serem demandadas por meio de celebração prévia, cujo pagamento será efetivado após a entrega dos serviços e relatórios de execução, conforme itens **5 – Transição de Serviços e Conhecimento**, **6 – Modelo de Faturamento** e **7 – Procedimento de Fiscalização e Pagamento dos Serviços** da **Especificação detalhada do objeto (1.1.1).**

Os serviços técnicos especializados em segurança da informação devem atender os seguintes requisitos mínimos:

Execução de horas estipuladas em Ordem de Serviço específica, sem garantia de quantidade mínima de execução, tratando-se apenas de uma estimativa de execução de serviços no escopo da solução de Serviços Gerenciados de Segurança, limitando-se, exclusivamente, aos seguintes casos:

- Elaboração de pareceres em segurança da informação;
- Análise e suporte de planos de melhoria de infraestrutura de segurança;
- Suporte a mudanças de arquitetura do ambiente computacional;
- Apoio na definição e implementação de mecanismos futuros de monitoramento e recursos de segurança;
- Desenvolvimento e implantação de indicadores de segurança não previstos;
- Orientação quanto ao procedimento de auditoria forense no ambiente computacional;
- Transferência de conhecimento por meio de workshops para questões especificas aplicadas às atuais soluções implementadas.

Execução de serviços por meio de Ordem de Serviço Técnico Especializado, previamente definida, documentada, protocolada e aprovada ao tempo necessário de atendimento.

Conclusão e validação de uma Ordem de Serviço Técnico Evolutivo somente após a entrega da documentação dos procedimentos.

4. Expectativa de Consumo

A CONTRATADA não se obriga a consumir nenhum dos quantitativos abaixo estipulados.

Para aqueles itens em que a medição é realizada por critérios quantitativos, tal valor será estipulado em uma ou mais Ordem de Serviço.

Para fins de faturamento de determinado período contratual, a quantidade a ser utilizada no cômputo da fatura será a quantidade presente na prestação de cada serviço no último dia do ciclo de faturamento em questão.

Conforme tabela abaixo, segue a expectativa de consumo:

Serviço	Unidade de Medição	Quantidade MENSAL
1. Serviço de gestão de vulnerabilidades	**Aplicações Web**: quantidade de URLs monitoradas	154
	Ativos de Rede: quantidade de IPs e/ou Dispositivos monitorados	2208
	Container: quantidade	130 deployments
2. Serviço de monitoramento de ataques cibernéticos (SIEM)	**Correlacionamento de Pacotes**: quantidade de Eventos por Segundo (EPS). A solução deverá monitorar uma quantidade de EPS definida por Ordem de Serviço e com a obrigação de suportar picos que excedam o quantitativo estipulado por até 8 dias no ciclo mensal de faturamento.	4000
	Detecção e resposta em endpoints: quantidade de Dispositivos monitorados	2059
3. Serviço de respostas aos incidentes de segurança e de privacidade	**Serviço Contínuo**: será fornecido de forma contínua, mensalmente e independe de qualquer métrica e deve obedecer ao respectivo Acordo de Nível de Serviço - ANS.	N/A
4. Serviço de inteligência aplicado à segurança da informação	**Serviço Contínuo**: será fornecido de forma contínua, mensalmente e independe de qualquer métrica e deve obedecer ao respectivo Acordo de Nível de Serviço - ANS.	N/A
5. Serviço de testes de invasão (PENTEST)	Hora – Homem (Mensal)	50
6. Serviços técnicos especializados	Hora – Homem (Mensal)	50

5. Transição de Serviços e Conhecimento

O escopo de serviços previsto no presente Termo de Referência engloba um amplo leque de temas/ambientes tecnológicos, técnicas e sistemas.

Comumente, há situações em que um determinado serviço precisa ser deslocado de um determinado contrato/prestadora para um novo contrato/contratada. Assim, a fim de assegurar a correta absorção dos serviços pela (nova) CONTRATADA, bem como a apropriada evolução da qualidade dos serviços prestados, estabelece-se que a prestação dos serviços descritos neste termo de referência será organizada nas seguintes etapas:

5.1. Iniciação: período após a assinatura do contrato, onde acontecem reuniões com outras contratadas e CONTRATANTE e tomada de conhecimento do ambiente tecnológico da CONTRATANTE.

5.2. Transição de serviços: período em que a CONTRATADA desempenhará as atividades de levantamento de dados inicial e documentação dos processos da outra contratada e do ambiente tecnológico necessárias para início da operação do ambiente por parte da CONTRATADA, documentar os elementos, sistemas e rotinas de transição, apresentando para a CONTRATANTE, que tem a prerrogativa de fazer sugestões e propor melhorias.

Nessa etapa, a CONTRATADA irá propor as soluções, quantitativos, esforços, equipe, para que a CONTRATANTE possa deliberar e emitir as respectivas Ordens de Serviço.

5.3. Transformação de serviços: período após o fim da transição em que a CONTRATADA inicia a operação e implantará as melhorias de processo e novas tecnologias necessárias para a evolução da qualidade dos serviços de TI previstos neste termo de referência. Basicamente, é o setup das ferramentas aprovadas.

5.4. Suporte continuado: período após a finalização das atividades de transformação dos serviços em que são remuneradas atividades rotineiras e atividades projetizadas solicitadas pela CONTRATANTE.

5.5. Transferência de conhecimento: etapa final do ciclo onde um novo movimento de transição está por vir. A contratada deve transferir o conhecimento, de forma completa e eficaz, para a CONTRATANTE e a outras partes por ela indicadas, de forma que haja plena continuidade dos serviços.

É importante observar que a documentação é exercício contínuo e decorrente da execução das atividades previstas no objeto contratual. A entrega da documentação é apenas transição do conhecimento acumulado.

A CONTRATADA deverá detalhar e repassar, conforme orientação da CONTRATANTE, todo o conhecimento técnico utilizado na prestação dos serviços, sem prejuízo da devida atualização da base de conhecimento ao longo de toda a execução contratual, da seguinte forma:

Transferência de conhecimento. Repasse de conhecimento a cada atualização do ambiente montado pela CONTRATADA quando da implantação de alterações na arquitetura existente:

Forma de transferência:

Fornecimento de subsídios tais como a disponibilização de toda documentação gerada a partir de modificação/atualização das soluções e serviços; manuais de instalação, configuração e operação do software em sua última versão; relatórios gerenciais e técnicos, de forma que a equipe técnica indicada pela CONTRATANTE obtenha todo o conhecimento necessário ao perfeito entendimento da solução, estando capacitados ao final do serviço contratado a manter os serviços.

Os documentos técnicos produzidos pela CONTRATADA, a respeito da prestação de serviço prevista neste documento, são de propriedade da CONTRATANTE, sendo seu conteúdo divulgado apenas com a expressa autorização desta.

Os dados gerados/armazenados nas ferramentas usadas pela CONTRATADA, na prestação dos respectivos serviços deverão ser exportados e entregues à CONTRATANTE. Em formato estruturado.

6. Modelo de Faturamento

O faturamento decorre do escopo e tipo de serviço prestado, com respectivos quantitativos e valores, dentro do período mensal.

A medição de cada serviço prestado deverá ocorrer no último dia do ciclo de faturamento.

Será emitida uma ou mais Ordens de Serviço (OS) para início da prestação dos serviços objeto deste contrato. A partir da emissão desta ordem de serviço se dará a contagem dos prazos de execução deste contrato, os quais ficam sujeitos aos respectivos Acordos de Níveis de Serviço e Sanções.

Para fins de remuneração os serviços são classificados em dois tipos de tarefas:

- **Rotineiras**: baseadas nas descrições e unidades de medição e fornecimento conforme explicitado em cada item de serviço;
- **Projetizadas**: aquelas previstas nos serviços previstos nos **itens 3.5** e **3.6** da **Especificação detalhada do objeto (1.1.1)**, a serem demandas mediante Ordem de Serviço específica, que descreverá o escopo e objeto do trabalho projetizado.

O aumento ou redução da quantidade de objetos para qualquer serviço deve ser sempre precedido de emissão de Ordem de Serviço, pela CONTRATANTE, de acordo com processo definido pela CONTRATANTE.

A CONTRATADA emitirá o relatório de serviços executados no período até o quinto dia útil do mês posterior à execução. O relatório terá como base de medição a situação do ambiente no último dia útil do mês de execução dos serviços. Será utilizado o modelo aprovado pela CONTRATANTE, para conferência e ateste dos serviços prestados;

Não haverá fracionamento dos quantitativos em razão da quantidade de dias úteis no mês. O relatório de serviços executados deverá demonstrar os quantitativos suportados de cada serviço na data de sua emissão.

O primeiro e o último mês do contrato serão faturados proporcionalmente à quantidade de dias de execução contratual.

A CONTRATADA deve, além da adequada prestação do serviço, providenciar, a cada ciclo de faturamento, os entregáveis especificamente descritos para cada um dos itens de serviços descritos no presente Termo de Referência.

Os entregáveis representam evidências da prestação dos serviços e são parte necessária para a realização dos procedimentos de ateste e pagamento pelo serviço prestado.

Remuneração de tarefas projetizadas:

Os serviços definidos nos itens 3.5. Serviço de testes de invasão e 3.6. Serviços técnicos especializados são de caráter projetizadas.

CONTRATANTE emitirá para cada nova demanda do tipo projetizada um Documento de Requisição de Estimativa de Atividade Projetizada (REAP) estabelecendo requerimentos, escopo das atividades, restrições e critérios de aceite.

A CONTRATADA deverá apresentar Estimativa Prévia de Atividade Projetizada (EPAP) para realização da tarefa estabelecida no Documento de Requisição de Estimativa de Atividade Projetizada (REAP), detalhando as macro atividades, a quantidade de horas-homem de serviço técnico especializado para cada macro atividade, premissas e prazo máximo para execução completa do escopo definido.

A CONTRATANTE revisará a estimativa prévia e emitirá Ordem de Serviço aprovando e dando início à prestação dos serviços delimitados no respectivo escopo.

A CONTRATANTE, a seu próprio critério, pode instituir um Comitê para deliberação e aprovação das estimativas EPAP e emissão da respectiva Ordem de Serviço.

O faturamento das atividades projetizadas ocorrerá após o aceite final pela CONTRATANTE, que será realizado após a encerramento e entrega do projeto, e corresponderá à quantidade total de horas-homem aprovadas quando da emissão da Ordem de Serviço.

Em caso de cancelamento do projeto por decisão da CONTRATANTE, a CONTRATADA será remunerada pró-rata pelos serviços executados até a data de notificação do encerramento do projeto mediante apresentação das evidências do trabalho executado.

O descrito neste artigo não se aplica caso o cancelamento do projeto decorra de má execução imputável à CONTRATADA.

A CONTRATANTE poderá a seu critério, para atender as suas necessidades, realizar revisões nas Ordens de Serviço emitidas, desde que devidamente motivadas, nos seguintes casos:

- Ajustes nos cronogramas do projeto;
- Mudança de escopo do projeto, ensejando ajuste no Documento de Requisição de Estimativa de Atividade Projetizada, assim como apresentação de nova Estimativa Prévia de Atividade Projetizada por parte da CONTRATADA;
- Ajustes devido a erros formais;
- Atrasos provocados por terceiros;
- Outros ajustes correlatos.

As ações serão executadas pela CONTRATADA a partir da emissão de Ordem de Serviço pela CONTRATANTE.

7. Procedimento de Fiscalização e Pagamento dos Serviços

O processo de faturamento observará a sequência:

Até o quinto dia útil de cada mês o preposto da CONTRATADA entregará ao Fiscal do Contrato o relatório de serviços executados, com detalhamento dos serviços efetivamente prestados no mês anterior, quantitativos de objetos dos serviços, métricas de qualidade alcançadas quanto aos Acordos de Níveis de Serviços (SLA) e, por conseguinte, valores cobrados;

O Fiscal do Contrato analisará o relatório e devolverá, em até 10 (dez) dias úteis, o relatório de serviços executados aprovado ou com indicação das correções a serem introduzidas, acompanhado do detalhamento dos valores glosados em razão do descumprimento dos Acordos de Níveis de Serviços (SLA), referentes ao mês;

No caso de aprovação do relatório dos serviços executados, o preposto da CONTRATADA providenciará a emissão da nota fiscal mensal, considerando os descontos apresentados;

No caso de não aprovação do relatório dos serviços executados e concordância do preposto da CONTRATADA com as correções informadas pelo fiscal do contrato da CONTRATANTE, o preposto da CONTRATADA atualizará o relatório de serviços executados e providenciará a emissão da nota fiscal mensal, considerando os descontos apresentados;

No caso de não aprovação do relatório de serviços executados e não concordância do preposto da CONTRATADA com as correções informadas pelo fiscal do contrato da CONTRATANTE, o preposto da CONTRATADA providenciará a emissão da nota fiscal mensal e o fiscal do contrato realizará o ateste contratual e sugerirá ao gestor do contrato a aplicação das glosas que considerar necessárias.

Após o ateste da respectiva Nota Fiscal, o processo administrativo entra na competência dos demais setores administrativos da contratada, que seguirá o rito definido em legislação específica.

8. Acordo de Nível de Serviço

Para garantir que a CONTRATADA preste um serviço de qualidade, são estabelecidas nesse Termo de Referência metas para o Acordo de Nível de Serviço - SLA. O descumprimento destas metas afetará o valor a ser faturado pelo serviço efetivamente prestado, sem prejuízo da aplicação de sanções pelo não cumprimento das obrigações contratuais.

Sempre que possível, quando não forem atingidos os níveis de serviços exigidos, a CONTRATANTE aplicará reduções no pagamento (glosas), de forma a retratar que a qualidade dos serviços recebidos não foi de acordo com a qualidade exigida em contrato.

As glosas serão calculadas e aplicadas:

- Sobre o valor do faturamento do mês referente ao serviço a ser glosado;
- Para fins desse cálculo não será considerado o faturamento proveniente de atividades projetizadas.

Essas glosas não excederão a 20% (vinte por cento) do valor total do faturamento do mês;

A aplicação das glosas definidas nesse Termo de Referência não exclui a aplicação das sanções e penalidades cabíveis.

Considerando o ciclo previsto no item **5. Transição de Serviços e Conhecimento** da **Especificação detalhada do objeto (1.1.1)**, para as tarefas rotineiras, pode-se perceber a seguinte sequência de acontecimentos:

1. Iniciação;

2. Transição de Serviços;
    a. Apresentação e aprovação de Ordens de Serviço
3. Transformação de Serviços;
4. Suporte continuado;
5. Transferência de Conhecimento;

Sempre que possível, uma comunicação oficial entre o fiscal do contrato e o preposto da CONTRATADA, iniciará a contagem dos prazos.

8.1. Durante a etapa de **Iniciação**, na qual a CONTRATADA passa a reunir-se com outras empresas contratadas, comprometendo-se a comparecer desde que:

- **Reuniões remotas** sejam agendadas com pelo menos **4 horas de antecedência**.
- **Reuniões ou Visitas presenciais**, sejam solicitadas com pelo menos **24 horas de antecedência**.

A etapa de Iniciação, ao todo, deverá durar, no máximo **10 dias úteis**.

8.2. Durante a etapa de **Transição de Serviços**, a CONTRATADA terá **15 dias úteis para propor as soluções técnicas e respectivas equipes** (observado o **Item 11 - Perfil Profissional** da **Especificação detalhada do objeto (1.1.1)**)

Antes do início da etapa seguinte (**Transformação de Serviços**), a CONTATANTE irá deliberar e em sendo o caso, aprovar as tantas Ordens de Serviço quantas forem necessárias para delimitar o escopo dos trabalhos.

8.3. A CONTRATANTE tem prazo de **10 dias úteis para aprovar ou solicitar adequação nas propostas** (situação em que seu prazo é devolvido);

8.4. Com a respectiva aprovação das Ordens de Serviço, a CONTRATANTE passa à etapa Transformação de Serviços, quando terá **15 dias úteis para configurar os ambientes, ferramentas e regras necessárias para que os objetivos delineados, para cada serviço previsto, sejam atingidos** e iniciar a prestação dos serviços propriamente dita.

8.5. Durante a etapa de **Suporte Continuado** (plena prestação rotineira dos serviços) deve-se atentar para os seguintes níveis:

- Salvo disposição em contrário, a disponibilidade das ferramentas e serviços rotineiros deverá ser de 99,9%.
- Todas as ferramentas utilizadas na prestação de serviços contínuos (por exemplo, correlação de pacotes) deverão fornecer relatórios de disponibilidade (mensais ou quando solicitados).
- Os períodos registrados como indisponíveis, mediante aprovação do líder de serviço da CONTRATANTE, poderão ser considerados disponíveis nos seguintes casos:
    - Decorrentes de janelas de mudanças autorizadas pela Contratante, e de acordo com o processo de mudança da Contratante.
    - Eventuais alarmes indevidos de indisponibilidade registrados na ferramenta de monitoração (falsos positivos), devidamente fundamentados.
- Os relatórios acima referidos devem ser entregues em até **5 dias úteis**.
- Os entregáveis específicos, previstos em cada serviço, devem ser fornecidos em **até 5 dias úteis** a contar da data do encerramento do ciclo ou da data solicitada.
- Sempre que necessária a implementação de novas regras, técnicas, configurações ou parametrizações de ferramentas, respostas automatizadas, seja de forma proativa ou reativa,

deve-se concluir a atualização em até **10 dias úteis**, a partir de comunicação específica, preferencialmente eletrônica.

A CONTRATADA só poderá faturar os serviços executados após o fechamento dos relatórios de serviços do mês.

A classificação dos chamados será realizada de acordo com as atuais práticas de mercado, a critério da CONTRATANTE, e formalizadas em reunião de trabalho específica, que será realizada até o final da etapa de transformação.

A CONTRATADA poderá se manifestar em relação à metodologia de classificação, sendo necessária a apresentação de critérios técnicos e objetivos, passíveis de comprovação por parte da CONTRATANTE.

A CONTRATANTE decidirá sobre a pertinência das alegações da CONTRATADA quanto à classificação dos chamados.

A CONTRATANTE poderá alterar a classificação dos incidentes e requisições de acordo com o impacto gerado.

Para requisições que necessitem de planejamento prévio, o prazo de execução deverá ser acordado entre as partes;

As horas de atendimento definidas nesta tabela serão contadas de acordo com o horário de cobertura definido para cada serviço.

Para incidentes que demandem investigação, de acordo com práticas de mercado, o prazo será acordado entre as partes.

8.6. Para tarefas projetizadas os prazos são definidos nas respectivas Ordens de Serviço, observado o item Multas sobre atividades projetizadas (subitem L em **Item 6.5. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS do respectivo Termo de Referência.**).

8.7. Para a etapa **Transferência de Conhecimento**, tem-se:

- Transferência final de conhecimentos sobre a execução e a manutenção dos serviços:
  - Responsável: CONTRATADA
  - Início: No mínimo 90 dias antes do encerramento contratual;
  - Fim: Dia anterior ao término do contrato.

- Disponibilização de todas as autenticações de acesso aos equipamentos, programas, suporte técnico, sistemas e documentos sob responsabilidade da CONTRATADA:
  - Responsável: CONTRATADA
  - Início: No mínimo 90 dias antes do encerramento contratual;
  - Fim: Dia anterior ao término do contrato;
  - Responsável: CONTRATADA
  - Início: Início da execução do contrato;
  - Fim: Término do contrato;

Para os itens 8.1, 8.2, 8.4, 8.5, 8.6 e 8.7 supra, aplicam-se exclusivamente sanções previstas no Item **6.5 - INFRAÇÕES E SANÇÕES ADMINISTRATIVAS** do texto do presente Termo de Referência

9. Ambiente Tecnológico

9.1. Tabela contendo serviços e respectivas tecnologias

Linha de serviço	**Tecnologias envolvidas**
Serviço de manutenção e suporte a usuários, aplicações, estações de trabalho e infraestruturas físicas de redes	Windows 7, 10 e 11
Serviço de manutenção e suporte a demais dispositivos de usuários.	Impressoras (Lexmark T654, HP T790 MFP E52645, HP E55040, Samsung CLP 775, Argox 214, FX, ALOS), Scanner (FUJITSU FI-6770 e AVISION AV176U), Telefone (Avaya 9608, BM12, H175)
Serviço de monitoração de TI	Zabbix 4 Grafana 6
Serviço de manutenção e suporte lógico a ativos de redes	Switches HP (5900, 5130, 5920, 11900), Juniper MX104, Cisco Access Point AIR-CAP1702I-Z-K9 e AIR-CAP2702I-Z-K9
Serviço de administração e suporte à infraestrutura de backup e de armazenamento	Storage HP (3PAR 7200), Storage Huawei (High-End CTRL01 e Hybrid CTRL01), HP Tape Library (MSL 4048 G3), Net Backup (MSL4048), file servers.
Serviço de administração e suporte à infraestrutura de datacenter	HP Tape Library (MSL 4048 G3), Net Backup (MSL4048), Storage HP (3PAR 7200), Storage Huawei (High-End CTRL01 e Hybrid CTRL01), Servidores DL360 GEN 10, Balanceador A10, controladora Wifi Cisco 5500, Gateway Avaya G450
Serviço de administração e suporte à infraestrutura de virtualização	VMWare 7 update 3 ESXi 7 update 3 Vcenter 7 update 3
Serviço de administração e suporte aos servidores Linux e Unix	CentOS 7 e 8 Ubuntu 20.04
Serviço de administração e suporte aos servidores Windows	Windows Server 2012, 2012 R2, 2019 e 2022
Serviço de administração e suporte à aplicações	Avaya CM 8.1 KVM 1.9 WDS NGINX 1.14 RKE/Rancher 1.23 IIS 8.5 Remoteapp OCS 7.4 Kubernetes 1.23
Serviço de administração e suporte à infraestrutura de banco de dados	SQL Server Standard 2016 MySQL 5.6.19 Community Server MariaDB 5.5

Serviço de administração e suporte à ferramentas de monitoração	Zabbix 4 Grafana 6 Prometheus
Serviço de administração e suporte à ferraemnta de gestão de identidades	Radius 10 (Windows Server 2019) AD, Office 365, LDAP e MFA
Serviço de administração e suporte às ferramentas de segurança da informação	Palo Alto 3260 Cilium Kaspersky 14.0.0.10902 Avaya SBC 8.1 WSUS
Serviço de administração e suporte às ferramentas de Service Desk e Gestão de Projetos e Portfólio	OTRS 6.4, Redmine 4.2, Gitlab 15.5 KVM 1.9
Serviço de administração e suporte de administração e suporte às ferramentas de colaboração	Gateway Avaya G450 Avaya Zenit 8.1 Avaya GPN4000 Avaya Breeze 8.1 Teams, Office 365 Sharepoint Moodle 3

9.2. Tabela contendo serviços e quantitativos atuais e estimados

	Quantitativo de objetos					
Linha de Serviço	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**
Serviço de manutenção e suporte a usuários, aplicações, estações de trabalho e infraestruturas físicas de redes	1289	1468	1456	1551	1653	1760
Serviço de manutenção e suporte a demais dispositivos de usuários.	1324	1341	1298	1298	1298	1298
Serviço de monitoração de TI	744	744	744	744	744	744
Serviço de manutenção e suporte lógico a ativos de redes	147	149	149	149	149	149
Serviço de administração e suporte à infraestrutura de backup e de armazenamento	135	195	207	259	325	407
Serviço de administração e suporte à infraestrutura de datacenter	40	47	41	41	41	41
Serviço de administração e suporte à infraestrutura de virtualização	6	14	8	8	8	8
Serviço de administração e suporte aos servidores Linux e Unix	71	107	121	137	155	175
Serviço de administração e suporte aos servidores Windows	59	72	77	88	101	116
Serviço de administração e suporte à aplicações	33	53	60	82	112	154
Serviço de administração e suporte à infraestrutura de banco de dados	17	18	20	22	24	26

Serviço de administração e suporte à ferramentas de monitoração	3	4	4	4	4	4
Serviço de administração e suporte à ferramenta de gestão de identidades	6	8	8	8	8	8
Serviço de administração e suporte às ferramentas de segurança da informação	6	10	10	20	20	20
Serviço de administração e suporte às ferramentas de Service Desk e Gestão de Projetos e Portfólio	5	7	8	8	8	8
Serviço de administração e suporte de administração e suporte às ferramentas de colaboração	11	13	9	2	2	2

10. Termos e Definições

10.1. ANS ou SLA – Acordo de Nível de Serviço ou Service Level Agreement;

10.2. Atendimento Remoto – Atendimento realizado por meio de telefone, e-mail, sistema ou outra forma remota, ainda que nas dependências da contratada (local de prestação presencial);

10.3. Atividade Projetizada - tarefas empreendidas, tempestivamente, para execução de serviço com resultado específico, com início e término preestabelecidos;

10.4. Atividade Rotineira - tarefas de periodicidade previamente definida para execução, ou pontuais conforme estabelecidos na descrição dos serviços neste Termo de Referência;

10.5. Ativo de TI - Bens de valor que a área de TI compra e/ou gerencia. Estes ativos podem ser software, hardware, sistemas ou serviços.

10.6. Prestação de serviço remoto – Serviço realizado fora das dependências da CONTRATANTE;

10.7. Preposto – Representante da CONTRATADA, aceito pela Administração, na execução do contrato.

11. Perfil Profissional

É responsabilidade da CONTRATADA selecionar e manter os profissionais adequados para os perfis abaixo elencados, bem como o respectivo suplente para os períodos de ausência do titular.

11.1. **Preposto**: profissional indicado pela CONTRATADA para servir de contato para tramites administrativos**.**

É o responsável pela coordenação operacional das atividades previstas nos projetos, de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução dos trabalhos. Deverá ter bons conhecimentos em gestão de projetos para garantir o controle sobre as atividades e projetos.
A CONTRATADA tem a prerrogativa de solicitar a substituição do preposto.

11.2. **Líder Técnico Geral**: profissional que conheça todos os serviços prestados.
Certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring).

Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);
Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação.
Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

O Líder Técnico Geral deverá ser exclusivo para o presente contrato e não deve integrar demais equipes.

11.3. **RED Team: deve possuir um líder e respectivo suplente (durante períodos de ausência) com o perfil abaixo.**

11.4. **Perfil Líder RED Team**
Certificações: LPIC 1, 2 e 3 ou CySA+ ou ISFS ou ECCouncil CEH ou CompTIA Pentest+.

Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);
Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação.
Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

O RED Team deverá ser dimensionado com outros profissionais, com formação pertinente e de forma a atender os requisitos de Nível de Serviço (**Item 8 – Acordo de Nível de Serviço** da **Especificação detalhada do objeto (1.1.1)**).

11.5. **Time Técnico Específico: atenderá de forma compartilhada ou não os demais serviços, atendidos os Níveis de Serviço** (**Item 8 – Acordo de Nível de Serviço** da **Especificação detalhada do objeto (1.1.1)**), **sendo necessário que o Líder Técnico Específico possua o perfil abaixo.**

11.6. **Líder Técnico Específico**: cada um dos serviços elencados deve possuir um Líder Técnico responsável, que pode ser compartilhado dentre mais de um dos respectivos serviços, atendidos ao Níveis de Serviço estipulados (**Item 8 – Acordo de Nível de Serviço** da **Especificação detalhada do objeto (1.1.1)**).

Certificações: ISFS (Information Security Foundation)

Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de

pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);
Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação.
Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

O Time Técnico Específico deverá ser dimensionado com outros profissionais, com formação pertinente e de forma a atender os requisitos de Nível de Serviço (**Item 8 – Acordo de Nível de Serviço** da **Especificação detalhada do objeto (1.1.1)**).

11.7. Profissional ISTM: encarregado de gerenciar o sistema de gestão dos eventos.

Certificações: ITIL v3 ou ISFS (Information Security Foundation)

Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);
Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação.
Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

OBSERVAÇÕES GERAIS SOBRE O PERFIL PROFISSSONAL: Os diversos serviços do edital são atendidos pelos profissionais descritos no item 4 supra (Time Técnico Específico), sendo compreendidos pelo Blue Team.
É necessário haver a devida segregação e distinção (incluída a não acumulação de tarefas e funções) entre os profissionais que integrem o perfil previsto no item 4 (Time Técnico Específico) e os profissionais que integram o item 3 supra (RED Team).

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns), conforme justificativa constante do Estudo Técnico Preliminar.

1.3. *O prazo de vigência da contratação é de trinta e seis meses (36 meses) contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133/2021.*

1.3.1. *O serviço é enquadrado como continuado tendo em vista que há operação de técnicas de segurança da informação no ambiente tecnológico da CONTRATANTE em regime contínuo, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.*

1.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (art. 6º, inciso XXIII, alínea 'b' da Lei n. 14.133/2021).

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudo Técnicos Preliminares – ETP.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO (art. 6º, inciso XXIII, alínea 'c')

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares – ETP.

3.2. O item 1 apresenta a descrição detalhada do objeto de contratação.

4. REQUISITOS DA CONTRATAÇÃO (art. 6º, XXIII, alínea 'd' da Lei nº 14.133/21)

4.1. SUSTENTABILIDADE

4.1.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os requisitos que se baseiam no Guia Nacional de Contratações Sustentáveis.

4.2. SUBCONTRATAÇÃO

4.2.1. Não será admitida a subcontratação do objeto contratual. Todavia, a CONTRATADA não está impedida de contratar ferramentas e respectivo suporte técnico para a prestação do serviço descrito no presente Termo de Referência.

4.3. *GARANTIA DA CONTRATAÇÃO*

4.3.1. *Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133/21, no percentual de 5% do valor contratual, conforme regras previstas no contrato.*

4.3.1. *A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 10 dias após a assinatura do contrato*

4.3.2. *Em caso opção pelo seguro-garantia, a parte adjudicatária terá prazo de um mês, contado da data de homologação da licitação, para sua apresentação, que deve ocorrer antes da assinatura do contrato.*

5. MODELO DE EXECUÇÃO CONTRATUAL (arts. 6º, XXIII, alínea "e" da Lei n. 14.133/2021).

5.1. Condições de execução

5.1.1. A execução do objeto seguirá a seguinte dinâmica:

5.1.1.1. Início da execução do objeto: ocorrerá em data estipulada em emissão de Ordem de Serviço genérica.

5.1.1.2. A execução contratual se dará conforme detalhado na especificação do objeto (Item 1.1.1);

5.1.1.3. Local e horário da prestação de serviço: o serviço será prestado em regime de 24 horas por dia, 7 dias por semana, durante a duração do contrato, de forma remota, mas sempre que necessário, profissionais da CONTRATADA deverão comparecer presencialmente, conforme descrito no objeto da contratação (Item 1.1.1)

6. MODELO DE GESTÃO DO CONTRATO (art. 6º, XXIII, alínea "f" da Lei nº 14.133/21)

6.1. 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. (Lei nº 14.133/2021, art. 115, caput).

6.2. 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. (Lei nº 14.133/2021, art. 115, §5º).

6.3. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa CONTRATADA 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 da CONTRATADA, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.4. Preposto:

6.4.1. A CONTRATADA designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

6.4.2. A CONTRATANTE poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a CONTRATADA designará outro para o exercício da atividade.

6.4.3. As comunicações entre o órgão ou entidade e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4.4. O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Rotinas de fiscalização contratual

6.5.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133/2021, art. 117, caput).

6.5.1.1. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133/2021, art. 117, §1º).

6.5.1.2. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência (Lei nº 14.133/2021, art. 117, §2º).

6.5.2. A CONTRATADA será obrigada a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados (Lei nº 14.133/2021, art. 119).

6.5.3. A CONTRATADA será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE (Lei nº 14.133/2021, art. 120).

6.5.4. Somente a CONTRATADA será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (Lei nº 14.133/2021, art. 121, caput).

6.5.4.1. A inadimplência da A CONTRATADA em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato (Lei nº 14.133/2021, art. 121, §1º).

6.5.5. A execução do contrato deverá ser acompanhada e fiscalizada de acordo com a atribuições elencadas no art. 120, do Decreto Municipal 62.100/2022, e demais previsões normativas relacionadas.

6.5.6. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas descritas nos itens abaixo, que compõem a **Especificação detalhada do objeto (1.1.1)**

6.5.6.1. Item 5. Transição de Serviços e Conhecimento

6.5.6.2. Item 6. Modelo de Faturamento

6.5.6.3. Item 7. Procedimento de Fiscalização e Pagamento dos Serviços

6.5.6.4. Item 8. Acordo de Nível de Serviço

6.6. Rotinas de gestão contratual

6.6.1. Constituem atividades a serem exercidas pela unidade administrativa responsável pela gestão de contratos todas a atribuições elencadas no art. 118, do Decreto Municipal 62.100/2022, e demais previsões normativas relacionadas.

6.7. Dos critérios de aferição e medição para faturamento

6.7.1. A avaliação da execução do objeto utilizará instrumento para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

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

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

6.7.2. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

6.7.2.1. O fiscal do contrato irá verificar se o prazo de entrega, as quantidades e a qualidade dos serviços encontram-se de acordo com o estabelecido no instrumento contratual;

6.7.2.2. O fiscal do contrato irá atestar a respectiva nota fiscal ou fatura e encaminhá-la à unidade responsável pela gestão de contratos.

6.7.3. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

6.7.3.1. Não produziu os resultados acordados;

6.7.3.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

6.7.3.3. Deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

6.8. Liquidação e pagamento

6.8.1. O prazo de pagamento será de 30 (trinta) dias, contados da data da entrega da Nota Fiscal ou Nota Fiscal Fatura, nos moldes da Portaria SF 170/2020 e 187/2020.

6.8.1.1. Serão aceitas como prova de regularidade, certidões positivas com efeito de negativas e certidões positivas que noticiem em seu corpo que os débitos estão judicialmente garantidos ou com sua exigibilidade suspensa.

6.8.2. A não apresentação de certidões negativas de débito, ou na forma prevista no subitem 9.3.1.1, não impede o pagamento, porém será objeto de aplicação de penalidade ou rescisão contratual, conforme o caso.

6.8.3. Caso venha ocorrer a necessidade de providências complementares por parte da CONTRATADA, a fluência do prazo será interrompida, reiniciando-se a sua contagem a partir da data em que estas forem cumpridas.

6.8.4. Caso venha a ocorrer atraso no pagamento dos valores devidos, por culpa exclusiva da Administração, a CONTRATADA terá direito à aplicação de compensação financeira, nos termos da Portaria SF nº 05, de 05/01/2012.

6.8.5. Para fins de cálculo da compensação financeira de que trata o item 9.3.4, o valor do principal devido será reajustado utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança para fins de compensação da mora (TR + 0,5% "pro-rata tempore"), observando-se, para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

6.8.6. O pagamento da compensação financeira dependerá de requerimento a ser formalizado pela CONTRATADA.

6.8.7. Antes do pagamento a contratante efetuará consulta ao Cadastro Informativo Municipal – CADIN MUNICIPAL, por força da Lei Municipal nº 14.094/2005 e Decreto nº 47.096/2006, do qual não poderá constar qualquer pendência.

6.8.8. Os pagamentos serão efetuados em conformidade com a execução dos serviços, mediante apresentação da(s) respectiva(s) nota(s) fiscal(is) ou nota(s) fiscal(is)/fatura, bem como de cópia reprográfica da nota de empenho, acompanhada, quando for o caso, do recolhimento do ISSQN – Imposto Sobre Serviços de Qualquer Natureza do mês de competência, descontados os eventuais débitos da CONTRATADA, inclusive os decorrentes de multas.

6.8.9. Na hipótese de existir nota de retificação e/ou nota suplementar de empenho, cópia(s) da(s) mesma(s) deverá(ão) acompanhar os demais documentos.

6.8.10. A CONTRATADA deverá apresentar, a cada pedido de pagamento, os documentos elencados na Portaria SF 170/2020.

6.8.11. Por ocasião de cada pagamento, serão feitas as retenções eventualmente devidas em função da legislação tributária.

6.8.12. O pagamento será efetuado por crédito em conta corrente, no BANCO DO BRASIL S/A, conforme estabelecido no Decreto nº 51.197/2010, publicado no DOC do dia 22 de janeiro de 2010.

6.8.13. Fica ressalvada qualquer alteração por parte da Secretaria Municipal da Fazenda, quanto às normas referentes ao pagamento de fornecedores.

6.8.14. Deve-se observar procedimentos descritos no item 7 da **Especificação detalhada do objeto (1.1.1)**

6.9. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

6.9.1. São aplicáveis as sanções e procedimentos previstos no Título IV, Capítulo I da Lei Federal nº 14.133/21 e Seção XI do Decreto Municipal nº 62.100/21.

6.9.1.1. As penalidades só deixarão de ser aplicadas nas seguintes hipóteses:

a) comprovação, anexada aos autos, da ocorrência de força maior impeditiva do cumprimento da obrigação; e/ou,

b) manifestação da unidade requisitante, informando que o ocorrido derivou de fatos imputáveis exclusivamente à Administração.

6.9.2. Ocorrendo recusa da adjudicatária em retirar/receber a nota de empenho, dentro do prazo estabelecido para contratação, sem justificativa aceita pela Administração, garantido o direito prévio de citação e da ampla defesa, serão aplicadas:

a) Multa no valor de 20% (vinte por cento) do valor do ajuste se firmado fosse;

b) Pena de impedimento de licitar e contratar pelo prazo de até 3 (três) anos com a Administração Pública, a critério da Prefeitura

6.9.2.1. Incidirá nas mesmas penas previstas neste subitem a empresa que estiver impedida de firmar o ajuste pela não apresentação dos documentos necessários para tanto.

6.9.3. As penalidades poderão ainda ser aplicadas em outras hipóteses, nos termos da Lei, garantido o direito prévio de citação e da ampla defesa.

6.9.4. Pela inexecução total ou parcial do objeto desta contratação, a CONTRATANTE pode aplicar à CONTRATADA as seguintes sanções:

a) Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado

b) Multa de 0,5% (cinco décimos por cento), por dia sobre o valor total do ajuste, em caso de atraso no início da execução dos serviços, limitada a incidência a 10 (dez) dias. Após 10 (dez) dias de atraso será considerada inexecução parcial do contrato.

c) Multa de 1 % (um por cento), por dia sobre o valor total do ajuste, em caso de atraso no início da execução dos serviços, limitada a incidência do 11º (décimo primeiro) ao 20º (vigésimo) dia. Após o vigésimo dia será considerada inexecução total do ajuste.

d) Multa de 2% (dois por cento), sobre o valor total do ajuste, por não manter as mesmas condições da contratação quanto a regularidade fiscal e trabalhista, e na reincidência será aplicado o dobro;

e) Multa de 1% (um por cento), por dia de atraso, sobre o valor total do ajuste, por deixar de apresentar garantia contratual nos termos estipulados na contratação (seja inicial, reforço ou por ocasião de prorrogação), observado o máximo de 20% (vinte por cento). O atraso superior a 20 (vinte) dias autorizará a CONTRATANTE a promover a rescisão do contrato;

f) Multa de 3% (três por cento), sobre o valor mensal do ajuste, por descumprimento de qualquer obrigação da CONTRATADA para a qual não haja penalidade específica, por ocorrência e, na reincidência, será aplicado o dobro.

a. A cada reincidência, sobre o mesmo tipo de ocorrência, adiciona-se 1% aos 3% descritos acima. Até o limite de 10%.
b. Se a ocorrência acontecer após 6 meses da última, do mesmo tipo, será considerada nova incidência em detrimento de reincidência.

g) Multa de 10% (dez por cento), sobre o valor total do ajuste, por inexecução parcial do contrato.

h) Multa de 20% (vinte por cento), sobre o valor total do ajuste, no caso de rescisão do acordo, por culpa da CONTRATADA, inclusive por inexecução total do contrato, devida e previamente demonstrada a falta cometida à CONTRATADA;

i) Multa de 30% (trinta por cento), sobre o valor total do contrato, por deixar de comunicar à Secretaria a ocorrência de incidente de segurança; deixar de cumprir determinação da Secretaria para corrigir deficiências nos processos de tratamento; realizar

transferência de dados da Secretaria a terceiros sem expressa autorização e deixar de cumprir determinação da Secretaria para o exercício de direito de titular de dados.

j) Multas específicas:

Para os casos de não atendimento, por parte da CONTRATADA, das etapas, marcos e prazos estipulados nos **itens 8.1, 8.2, 8.4, 8.5, 8.6 e 8.7** da **Especificação detalhada do objeto (1.1.1)**, de acordo com a tabela abaixo:

Item	Descrição	Multa
8.1	Não atendimento aos prazos da etapa Iniciação	R$ 5.000,00
8.2	Não apresentação da proposta de solução	R$ 30.000,00 mais R$ 1.000 para cada dia de atraso
8.4	Não conclusão dos ambientes necessários para os serviços rotineiros	R$ 30.000,00 mais R$ 1.000 para cada dia de atraso
8.5	Não cumprimento dos prazos acerca dos entregáveis (relatórios e congêneres)	R$ 500,00 por dia de atraso
8.5	Não cumprimento da implementação das regras, parametrizações, configurações de ferramentas e congêneres	R$ 1.000,00 por dia de atraso
8.6	Não cumprimento do disposto em OS específica	Ver item **Multas sobre atividades projetizadas** abaixo (L)
8.7	Não cumprimento do item 8.7 no prazo estipulado	R$ 10.000,00 por dia de atraso
8.7	Não cumprimento do item 8.7	R$ 500.000,00

Dado que a documentação prevista no item 8.7 deve ser produzida ao longo da execução contratual, a CONTRATADA deverá apresentar a 180 dias da conclusão do contrato, proposta de documentação a ser entregue ao final do mesmo.

k) Multas aplicadas sobre o faturamento mensal das atividades rotineiras, nos seguintes percentuais:

a. 0,2% (dois décimos por cento) por dia de atraso, pela não substituição de profissional em até 30 dias corridos, quando requisitado pela CONTRATANTE.
b. 0,2% (dois décimos por cento), por dia, por linha de serviço, por profissional que não atenda às exigências do **Item 11 - Perfil Profissional** da **Especificação detalhada do objeto (1.1.1).**
c. 0,2% (dois décimos por cento), por dia de atraso, pelo não cumprimento do prazo de 15 (quinze) dias para iniciar a prestação dos serviços descritos em ordem de serviço, a partir de sua emissão.

l) Multas sobre atividades projetizadas:

Para os casos de não atendimento dos prazos, de acordo com a tabela abaixo:

Atividade	Tempo de Atendimento	Multa Aplicável
Confecção da Estimativa Prévia de Atividade Projetizada	Até 10 (dez) dias úteis após o envio da requisição.	R$250 por dia útil de atraso.

Entrega final das atividades definidas na Atividade Projetizada	De acordo com o prazo acordado durante a emissão da OS (em dias úteis)	5% sobre o valor da OS acrescido de 0,5% por cada dia útil de atraso, até o valor total da OS

m) **Glosas**: para as atividades em suporte continuado (Item 8.5 da **Especificação detalhada do objeto – 1.1.1**) aplicam-se as glosas conforme abaixo:

Incidentes/ Requisição	Descrição	Tempo para resolução	Glosa aplicável
Severidade 1	Serviço indisponível para grande número de usuários e/ou com alta degradação de performance. Serviço indisponível para o público externo (contribuintes, cidadãos, etc.).	1 hora	2% + (0,8% para cada item - incidente ou resolução - fora da SLA e por dia de atraso na resolução)
Severidade 2	Serviço degradado, com risco iminente de indisponibilidade ou indisponível. Incidentes relacionados a usuários de alta prioridade (limitado a 3% dos usuários).	4 horas	2% + (0,3% para cada item - incidente ou requisição - fora da SLA e por dia de atraso na resolução)
Severidade 3	Serviço apresentando problemas sem indisponibilidade ou degradação de performance para os usuários, eventos de alertas proativos sem impacto de negócios.	6 horas	2% + (0,1% para cada item - incidente ou requisição - fora da SLA e por dia de atraso na resolução)
Rotineiro	Operações das ferramentas em geral tais como configuração de regras, parametrização de ferramentais, criação e/ou configurações de usuários	12 horas	2% + (0,05% para cada requisição fora da SLA e por dia de atraso)

6.9.5. As sanções são independentes e a aplicação de uma não exclui a das outras, quando cabíveis.

6.9.6. Caso a CONTRATANTE releve justificadamente a aplicação da multa ou de qualquer outra penalidade, essa tolerância não poderá ser considerada como modificadora de qualquer condição contratual, permanecendo em pleno vigor todas as condições da contratação.

6.9.7. Das decisões de aplicação de penalidade, caberá recurso nos termos do artigo 161 da Lei Federal nº 14.133/21, observados os prazos nele fixados.

6.9.8. Os procedimentos de aplicação das penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar e contratar serão conduzidos por comissão, nos termos do artigo 158, "caput" e § 1º, da Lei Federal nº 14.133, de 2021.

6.9.9. São aplicáveis à presente contratação e ao ajuste dela decorrente no que cabível for, inclusive, as sanções penais estabelecidas na Lei Federal nº 14.133/21.

6.9.10. 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).

6.9.11. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela CONTRATANTE à CONTRATADA, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

6.9.12. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

7.1. Forma de seleção e critério de julgamento da proposta

7.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

7.2. Exigências de habilitação

7.2.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

7.2.1.1. Habilitação jurídica

7.2.1.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

7.2.1.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede; Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

7.2.1.1.3. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

7.2.1.1.4. Sociedade empresária estrangeira*:* portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

7.2.1.1.5. *Sociedade simples:* inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

7.2.1.1.6. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

7.2.1.1.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

7.2.1.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

7.2.1.2. Habilitação fiscal, social e trabalhista

7.2.1.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

7.2.1.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à

Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

7.2.1.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

7.2.1.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

7.2.1.2.5. Prova de inscrição no cadastro de contribuintes Municipal ou relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

7.2.1.2.6. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

7.2.1.2.7. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

7.2.1.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal**.**

7.2.1.3. Qualificação Econômico-Financeira

7.2.1.3.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

7.2.1.3.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

7.2.1.4. Qualificação técnica

7.2.1.4.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;

7.2.1.4.2. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

7.2.1.4.2.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

7.2.1.4.2.1.1. Serviços de segurança de tecnologia da informação para clientes que possuam pelo menos 1000 ativos de rede.

7.2.1.4.2.1. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

7.2.1.4.2.2. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

7.2.1.4.2.3. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

8. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

8.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas.

8.1.1. Para o valor estimado total da contratação será considerada a pesquisa de preço realizada pela Divisão de Compras e Contratos.

8.1.2. A estimativa de preços informada no Estudo Técnico Preliminar refere-se a uma pesquisa prévia inicial, e não servirá como base para reserva orçamentária.

9. ADEQUAÇÃO ORÇAMENTÁRIA

9.1. A indicação da dotação orçamentária fica postergada para o momento da assinatura do contrato ou instrumento equivalente.

9.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

São Paulo, 06 de junho de 2023.

_____

Identificação e assinatura do servidor responsável

CIDADE DE SÃO PAULO
FAZENDA

Estudo Técnico Preliminar

Unidade Solicitante: SF/COTEC/DISEG

Responsável pela Elaboração: Wilson Souza Lima Neto

Nº Processo SEI: 6017.2023/0033846-3

Data da Elaboração: 23/05/2023

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

Contratação de empresa especializada em serviços relacionados à temática de Segurança da Informação, principalmente no que diz respeito à definição, operação, monitoramento e uso de ferramentas para prevenção, detecção e resposta a eventos e incidentes de Segurança da Informação, no ambiente tecnológico da Secretaria da Fazenda do município de São Paulo, mais precisamente, o que segue:

- Serviço de gestão de vulnerabilidades;
- Serviço de monitoramento de ataques cibernéticos (SIEM);
- Serviço de respostas aos incidentes de segurança e de privacidade;
- Serviço de prevenção contra vazamento de dados (DLP);
- Serviço de controle de acesso à rede (NAC);
- Serviço de descoberta e mapeamento de dados pessoais e sensíveis;
- Serviço de inteligência aplicada à segurança;
- Serviço de teste de invasão (PENTEST);
- Serviços técnicos especializados.

Enquanto órgão arrecadador da Prefeitura de São Paulo, é de relevante importância o zelo e proatividade em evitar que incidentes de segurança da informação possam comprometer o fornecimento de serviços ao público interno/externo, bem como gestão da receita e do tesouro municipal, realizados por meio de sistemas de informação. Paralelamente, a Lei Geral de Proteção de Dados adiciona novos elementos que destacam ainda mais a necessidade pelo cuidado no tratamento de dados pessoais e/ou dados sensíveis/sigilosos.

2. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO

A contratação encontra-se respaldo no planejamento de TIC da Secretaria para o exercício de 2023 (PDSTIC/2023).

3. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

3.1. A prestação do serviço compreende a operação contínua e cotidiana das ferramentas e mecanismos de segurança da informação e, principalmente, soluções para situações reais de emergência, crise, ataques, vazamentos de informações e eventos correlatos.

3.2. O prazo de vigência do contrato será de 36 (trinta e seis) meses a contar da data de sua assinatura.

3.3. É responsabilidade da CONTRATADA a utilização, a instalação, a configuração e a manutenção da solução (ainda que em formato *on-premise* ou combinação de formatos), bem como licenças, adaptações acessórias, equipamentos e insumos acessórios à prestação do serviço.

3.4. É responsabilidade da CONTRATANTE a disponibilização de elementos estruturais e pressupostos básicos (notadamente fora do escopo do serviço), mas imprescindíveis para tal, tais como para o funcionam do espaço físico, energia elétrica e link de internet.

3.4.1. Insumos de instalação, tais como ferramentas, fiação, mão de obra básica e congêneres, necessários para interligar a estrutura da CONTRATANTE ao serviço prestado pela CONRATADA, será de responsabilidade da CONTRATADA.

3.5. Todos os softwares não podem constar, no momento da apresentação da proposta técnica, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida.

3.6. Deve-se englobar a alocação de softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

3.7. Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada, e estarem cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os softwares fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante/mantenedor.

3.8. Sempre que necessário, deverão fazer parte do fornecimento os servidores físicos necessários, obedecendo as especificações mínimas recomendadas pelo fabricante, assim como sistemas operacionais, sistemas de virtualização e softwares complementares para a completa instalação do sistema, atendendo a todas as características solicitadas, podendo a contratante ceder espaço de alocação no datacenter mediante prévia análise.

3.9. Não deve haver incompatibilidade dentre as soluções tecnológicas fornecidas pela CONTRATADA.

4. ESTIMATIVAS DAS QUANTIDADES A SEREM CONTRATADAS

Vide item 6

5. LEVANTAMENTO DE MERCADO

A análise e adequação entre a necessidade da Secretaria, sua demanda e respectiva oferta de mercado, com levantamento prévio e estimativo de custos e valores, pôde ser feita mediante análise de contratações similares em outros órgãos e entidades, de forma a embasar o presente Estudo Técnico Preliminar:

SPTrans: https://sistemas.sptrans.com.br/licitlovnew/hilicwebok.aspx?INS,,,,,,24,10,2022,0,0,0,,,,,,

Sebrae SP (Escopo Nacional): https://www.scf3.sebrae.com.br/portalcf/Licitacoes/Detalhe?Id=9670

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

A estimativa de preços informada neste instrumento refere-se a uma pesquisa prévia inicial, e não servirá como base para reserva orçamentária, quando deverá ser considerada a pesquisa de preços da Divisão de Compras e Contratos.

Valor estimado da CONTRATAÇÃO: **(R$): 7.413.858,00**

CÁLCULO DA ESTIMATIVA DOS PREÇOS

1. Serviço de gestão de vulnerabilidades			**Qtd**	**R$ Mensal**
Tipo	Medição	Preço Unitário	Unidades	
Aplicações Web	URL	R$ 215,00	154	R$ 33.110,00
Ativos de Rede	Ips/Dispositivos	R$ 16,30	2.208	R$ 35.990,40
Containers	Imagem de Container	R$ 26,17	130	R$ 3.402,10
				R$ 72.502,50
2. Serviço de monitoramento de ataques cibernéticos			**Qtd**	**R$ Mensal**
Tipo	Medição	Preço	Unidades	
Correlacionamento de pacotes	EPS	R$ 10,46	4.000	R$ 41.840,00
Detecção e resposta em Endpoint	Dispositivo	R$ 12,00	2.059	R$ 24.708,00
				R$ 66.548,00
3. Serviço de respostas aos incidentes de segurança e de privacidade			**Qtd**	**R$ Mensal**
Tipo	Medição	Preço	Unidades	

Resposta Incidentes	Valor Mensal	R$ 5.690,00	1	R$ 5.690,00
				R$ 5.690,00
4. Serviço de inteligência aplicado à segurança			**Qtd**	**R$ Mensal**
Tipo	Medição	Preço	Unidades	
Monitoramento	Valor Mensal	R$ 26.000,00	1	R$ 26.000,00
				R$ 26.000,00
5. Serviços de Teste de Invasão			**Qtd**	**R$ Mensal**
Tipo	Medição	Preço		
Reserva de Horas	Hora Homem	R$ 352,00	50	R$ 17.600,00
				R$ 17.600,00
6. Serviços técnicos especializados			**Qtd**	**R$ Mensal**
Tipo	Medição	Preço		
Reserva de Horas	Hora Homem	R$ 352,00	50	R$ 17.600,00
				R$ 17.600,00
			Mensal	**R$ 205.940,50**
			Anual	**R$ 2.471.286,00**
			Contrato	**R$ 7.413.858,00**

OBS.: Os quantitativos apresentados na presente tabela refletem as necessidades reais da Secretaria da Fazenda do município de São Paulo e os respectivos valores, decorrem de levantamento de mercado de serviços similares (principalmente no edital do Sebrae – Ver Item 5 supra), com eventual diferença no escopo, mas, principalmente, quantitativos diferentes em decorrência do porte das respectivas contratações, com o mero intuito, no escopo do ETP, de estimar valores para análise da viabilidade de contratação.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A contatação compreenderá o serviço, de forma que as ferramentas, sistemas e insumos são responsabilidade da contratada, com a qualidade regulada por Acordo de Nível de Serviço.

Utilização de técnicas, ferramentas, pessoas especializadas, boas práticas e frameworks para a prestação dos seguintes serviços, de forma integrada:

1. Gestão de Vulnerabilidades
1.1. Descrição: varredura ativa de vulnerabilidades de todos os itens (aplicações ou ativos de rede, containers) devendo ser capaz de analisar toda a infraestrutura de TI.

1.2. Objetivo a ser atingido: identificar, de forma proativa e recorrente, possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da SF, bem como a gestão de vulnerabilidade e seus respectivos atributos.

2. Monitoramento de Ataques Cibernéticos
2.1. Descrição: monitoramento contínuo e ininterrupto de ataques cibernético, mediante solução de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura.

2.2. Objetivo a ser atingido: registro e tratamento de eventos de segurança da informação, os quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo a um processo cíclico e rigoroso de gestão de eventos.

3. Resposta aos incidentes de Segurança/Privacidade
3.1. Descrição: analisar, remediar, conter e documentar os eventos/incidentes de segurança da informação, como ainda, fornecer a devida orientação técnica à contratante e aos demais prestadores de serviços correlatos, na obtenção da solução para incidentes, bem como implementar respostas automatizadas a determinados eventos.

3.2. Objetivo a ser atingido: oferecer as respostas (preferencialmente automatizadas) aos incidentes de segurança da informação, nos quais se incluem eventos relacionados à quebra da privacidade de informações pessoais e sensíveis, com a conseguinte restauração do ativo/serviço/processo.

4. Prevenção contra Vazamento de Informações
4.1. Descrição: prevenção contra vazamento de informações, mediante identificação de dados sensíveis em endpoints e uso de ferramenta para impedir sua transmissão para meios externos não autorizados e prestar apoio consultivo para implantar as diretrizes de SF.

4.2. Objetivo a ser atingido: evitar o tráfego não autorizado de dados sigilosos, pessoais e/ou sensíveis.

5. Controle de Acesso à Rede
5.1. Descrição: fornecer, operar e suportar solução de controle de acesso à rede da SF, por meio de processo contínuo de detecção e categorização de dispositivos de infraestrutura de redes.

5.2. Objetivo a ser atingido: detectar e controlar atividades de switches, roteadores e outros dispositivos de redes, para evitar acessos ilegítimos, bem como gerenciar mecanismos de autenticação/autorização de acesso à rede por usuários diversos.

6. Descoberta/Mapeamento de dados pessoais/sensíveis
6.1. Descrição: descoberta e mapeamento automatizados de dados pessoais e sensíveis, sejam estes estruturados, bem como não estruturados, por meio de console unificado, mediante definição de escopo pela SF.

6.2. Objetivo a ser atingido: localizar objetivamente o dado, seu formato, classificação e localização, permitindo o tratamento adequado.

7. Serviço de Inteligência
7.1. Descrição: fazer buscas contínuas em Deep e Dark web sobre SF e pessoas por ela definidas, links falsos, documentos falsos, urls parecidas com as oficiais, que possam induzir fraudes, bem como a retirada "takedown" (independente da localidade em que se situa) dos respectivos endereços, endpoints, links, domínios e congêneres junto às empresas e aos órgãos competentes.

7.2. Objetivo a ser atingido: buscar, de forma eficaz e proativa, dados ilegítimos, fraudes e/ou vazamentos de dados e credenciais que envolvam SF em suas funções institucionais e pessoas que integrem seu respectivo quadro de profissionais.

8. Testes de Invasão
8.1. Descrição: uso de técnicas e ferramentas especificas (estáticas ou dinâmicas) para tentar obter acesso não autorizado e privilegiado aos ativos e informações, definidos por SF.

8.2. Objetivo a ser atingido: identificar, mapear, documentar, controlar e auxiliar na correção e, em sendo o caso, corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica e de segurança da informação.

9. Serviço Técnico Especializado
9.1. Descrição: serviços técnicos especializados e projetizados, para necessidades correlatas, novas implementações e/ou suporte de soluções de segurança da informação, durante o período de execução do contrato, desde que não conflitam ou pertençam ao objeto já estabelecido no presente termo de referência.

9.2. Objetivo a ser atingido: suprir necessidade correlata ou derivada, de temática associada à execução contratual.

8. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Considerando-se uma operação de **Security Operations Center – SOC**, que demanda uma atuação integrada de várias tecnologias para cada um dos serviços elencados no item 6, para fins de operação, resposta aos incidentes de segurança e proteção dos sistemas e ativos tecnológicos da Secretaria, sugere-se a não adoção do parcelamento do objeto.

9. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

Pretende-se assegurar e manter a disponibilidade, confidencialidade e integridade dos dados e infraestrutura tecnológica de SF, detectando proativamente as ameaças e fortalecendo as defesas cibernéticas

de forma tempestiva, mediante equipe especializada, como ainda a remediação, mitigação e contingência de dados decorrentes de eventuais ataques.

10. PROVIDÊNCIAS A SEREM ADOTADAS

Não há necessidade de adoção de providência para a presente aquisição, além das previstas nos respectivos instrumentos licitatórios e contratuais.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

A contratação correlata/interdependente é a do **NOC – Network Operations Center** (Contrato 21/2018 SEI 6017.2018-0017248-5), responsável pela operação e manutenção da infraestrutura, bem como outras eventuais contratações correlatas e/ou posteriores.

12. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS

Em decorrência de tratar-se de operação tecnológica, não foi identificado impacto ambiental direto.

13. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO

Diante das informações trazidas por esse estudo preliminar, vislumbra-se que é necessário proteger os ativos de dados e sistemas da Secretaria, tendo em vista o tratamento de dados pessoais, sigilosos, fiscais, bem como a infraestrutura que suporta a atividade arrecadatória do município, em decorrência da crescente onda de ataques cibernéticos e da possibilidade e viabilidade orçamentária para a contatação desse tipo específico de serviço.

São Paulo, datado e assinado digitalmente.

_____

Identificação e assinatura do servidor responsável

CIDADE DE SÃO PAULO
FAZENDA

PREGÃO ELETRÔNICO SF Nº 17/2023
TIPO DE LICITAÇÃO: MENOR PREÇO TOTAL
PROCESSO ELETRÔNICO Nº. 6017.2023/0033846-3
OBJETO: Contratação de serviços de Segurança da Informação (SOC – Security Operations Center), pelo período de 36 meses, conforme condições e exigências estabelecidas no Termo de Referência – Anexo II.

ANEXO III – PROPOSTA DE PREÇOS

A (empresa)..... inscrita no CNPJ sob nº ....., estabelecida na....., nº....., telefone nºs....., e-mail....., propõe a execução dos serviços descritos no Termo de Referência – Anexo II, nos seguintes preços e condições:

ITEM	OBJETO	TIPO	UNIDADE DE MEDIÇÃO	QTDE MENSAL	VALOR UNITÁRIO	VALOR MENSAL	VALOR PARA 36 MESES
1	Serviço de gestão de vulnerabilidades	Aplicações Web	URL	154	R$...	R$...	R$...
		Ativos de Rede	Ips/Dispositivos	2.208	R$...	R$...	R$...
		Containers	Imagem de Container	130	R$...	R$...	R$...
2	Serviço de monitoramento de ataques cibernéticos	Correlacionamento de pacotes	EPS	4.000	R$...	R$...	R$...
		Detecção e resposta em Endpoint	Dispositivo	2.059	R$...	R$...	R$...
3	Serviço de respostas aos incidentes de segurança e de privacidade	Resposta Incidentes	UNIDADE	1	R$...	R$...	R$...
4	Serviço de inteligência aplicado à segurança	Monitoramento	UNIDADE	1	R$...	R$...	R$...
5	Serviços de Teste de Invasão	Reserva de Horas	Hora Homem	50	R$...	R$...	R$...
6	Serviços técnicos especializados	Reserva de Horas	Hora Homem	50	R$...	R$...	R$...
VALOR TOTAL PARA 36 MESES							R$...(por extenso)

- ✓ Todos os impostos, despesas e encargos devidos para a correta execução do contrato estão inclusos nos preços, em conformidade com o estatuído no Edital e seus Anexos.
- ✓ **VALIDADE DA PROPOSTA**: ..... dias corridos contados a partir da data da apresentação da proposta (NÃO INFERIOR A 60 DIAS CORRIDOS).
- ✓ Para efeito de pagamento informamos os dados bancários: Banco do Brasil, Agência _____, Conta Corrente _____, em atendimento ao Decreto nº 51.197/2010.

LOCAL E DATA

Representante Legal/Procurador
(Nome completo, cargo ou função e assinatura do representante legal/procurador)

CIDADE DE
SÃO PAULO
FAZENDA

PREGÃO ELETRÔNICO SF Nº 17/2023
TIPO DE LICITAÇÃO: MENOR PREÇO TOTAL
PROCESSO ELETRÔNICO Nº. 6017.2023/0033846-3
OBJETO: Contratação de serviços de Segurança da Informação (SOC – Security Operations Center), pelo período de 36 meses, conforme condições e exigências estabelecidas no Termo de Referência – Anexo II.

ANEXO IV
MODELO REFERENCIAL DE DECLARAÇÕES
(PAPEL TIMBRADO DA EMPRESA)
(APRESENTAÇÃO OBRIGATÓRIA PARA TODAS AS LICITANTES)

A _____inscrita no CNPJ sob nº _____, por intermédio de seu representante legal o(a) Sr(a)._____, portador(a) da Carteira de Identidade nº_____ e do CPF nº _____ DECLARA:

1) para fins do disposto no inciso VI do art. 68 da Lei Federal nº 14.133/21, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, salvo, a partir de 14 anos, na condição de aprendiz;

2) que, até a presente data, inexistem fatos impeditivos para a sua habilitação no presente processo licitatório, inclusive condenação judicial na proibição de contratar com o Poder Público ou receber benefícios ou incentivos fiscais ou creditícios, transitada em julgada ou não desafiada por recurso com efeito suspensivo, por ato de improbidade administrativa, estando ciente da obrigatoriedade de declarar ocorrências posteriores;

3) que não se encontra declarada inidônea, nem suspensa ou impedida de licitar e contratar com a Administração Pública.

4) que observou e atende plenamente aos requisitos previstos aos parágrafos §1º, §2º, §3º do art. 4º da Lei Federal nº 14.133/21 (aplicável a ME/EPP);

5) que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na CF/88, leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, sob pena de desclassificação.

6) que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social.

7) Não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos II e IV do art. 1º e no inciso III do art. 5º da CF/88.

8) Que, em se tratando de microempresa, empresa de pequeno porte, que cumpre os requisitos estabelecidos no art. 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento estabelecido em seus artigos. 42 a 49.

9) Tenho conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;

LOCAL E DATA

Representante Legal/Procurador
(Nome completo, cargo ou função e assinatura do representante legal/procurador)

PREGÃO ELETRÔNICO SF Nº 17/2023
TIPO DE LICITAÇÃO: MENOR PREÇO TOTAL
PROCESSO ELETRÔNICO Nº. 6017.2023/0033846-3
OBJETO: Contratação de serviços de Segurança da Informação (SOC – Security Operations Center), pelo período de 36 meses, conforme condições e exigências estabelecidas no Termo de Referência – Anexo II.

ANEXO V
MODELO REFERENCIAL DE DECLARAÇÃO DE NÃO CADASTRAMENTO E INEXISTÊNCIA DE DÉBITOS PARA COM A FAZENDA DO MUNICÍPIO DE SÃO PAULO

A empresa _____inscrita no CNPJ sob nº _____, por intermédio de seu representante legal, Sr._____, portador(a) da Carteira de Identidade nº_____ e do CPF nº _____ DECLARA, sob as penas da Lei, que não está inscrita no Cadastro de Contribuintes Mobiliários do Município de São Paulo, bem assim que não possui débitos para com a Fazenda deste Município.

LOCAL E DATA

Representante Legal/Procurador
(Nome completo, cargo ou função e assinatura do representante legal/procurador)