TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

EDITAL DE PREGÃO ELETRÔNICO Nº 13/2026

Número da licitação no ComprasGov: 90013/2026

PROTOCOLO SEI nº 0090885-81.2023.8.16.6000

O Tribunal de Justiça do Estado do Paraná torna público aos interessados que realizará licitação para contratar o objeto abaixo descrito:

OBJETO	**SOLUÇÃO DE TI CONSISTENTE EM SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA (MSS), COM PRESTAÇÃO CONTÍNUA E SOB DEMANDA, APLICADOS AO AMBIENTE TECNOLÓGICO DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ, PELO PERÍODO DE 36 (TRINTA E SEIS) MESES PRORROGÁVEL ATÉ O LIMITE LEGAL**
CRITÉRIO DE JULGAMENTO	**MENOR PREÇO**
MODO DE DISPUTA	**ABERTO**
LOCAL DA SESSÃO	https://www.gov.br/compras/ UASG 926415 - Tribunal De Justiça Estado Do Paraná Nº da licitação no ComprasGov: 90013/2026
ACOLHIMENTO DE PROPOSTAS	**Início:** dar-se-ia 23/06/2026, dar-se á 02/10/2026 **Fim:** momento de abertura da sessão
ABERTURA DA SESSÃO PÚBLICA	Dar-se-ia 09/07/2026, dar-se-á 21/10/2026 às 13:00 horas (Horário de Brasília – DF) *Na hipótese de não haver expediente nessa data, realizar-se-á no primeiro dia útil subsequente*
PRAZO PARA IMPUGNAÇÃO	Até 03 (três) dias úteis antes da data de abertura da licitação

O edital, as especificações e os projetos estarão disponíveis gratuitamente às interessadas nos sites www.tjpr.jus.br/editais, www.pncp.gov.br e www.gov.br/compras.

Para download do aplicativo ComprasGov utilize o QR Code ao lado ou link abaixo.

http://onelink.to/comprasgovbr

Horário de atendimento TJPR: das 12:00 (doze) às 18:00 (dezoito) horas dos dias úteis.
E-mail: licit@tjpr.jus.br
Telefones: (41) 3250-6541, (41) 3250-6542
WhatsApp: (41) 3250-6541 - QR Code ao lado ou o link abaixo.

https://wa.me/message/2DOWV5UMLT4SB1

SUMÁRIO

CAPÍTULO 01 – DA LEGISLAÇÃO APLICÁVEL 3
CAPÍTULO 02 – DO OBJETO 3
CAPÍTULO 03 – DO PREÇO MÁXIMO E DA DOTAÇÃO ORÇAMENTÁRIA 3
CAPÍTULO 04 – DA IMPUGNAÇÃO DO EDITAL E DA OBTENÇÃO DE ESCLARECIMENTOS 3
CAPÍTULO 05 – DO CREDENCIAMENTO 3
CAPÍTULO 06 – DA PARTICIPAÇÃO 4
CAPÍTULO 07 – DO CADASTRAMENTO DAS PROPOSTAS INICIAIS 5
CAPÍTULO 08 – DA ABERTURA DA SESSÃO E CLASSIFICAÇÃO DAS PROPOSTAS 6
CAPÍTULO 09 – DA FORMULAÇÃO DE LANCES 7
CAPÍTULO 10 – DA NEGOCIAÇÃO 9
CAPÍTULO 11 – DO ENVIO DA PROPOSTA RECOMPOSTA E DOCUMENTOS COMPLEMENTARES 9
CAPÍTULO 12 – DO JULGAMENTO DA PROPOSTA 10
CAPÍTULO 13 – DA HABILITAÇÃO 12
CAPÍTULO 14 – DAS DISPOSIÇÕES GERAIS DA HABILITAÇÃO 16
CAPÍTULO 15 – DOS RECURSOS 16
CAPÍTULO 16 – DA CONTRATAÇÃO 17
CAPÍTULO 17 – DA EXECUÇÃO, FISCALIZAÇÃO, GESTÃO, RECEBIMENTO DO OBJETO E DO PAGAMENTO 17
CAPÍTULO 18 – DA LEI ANTICORRUPÇÃO 19
CAPÍTULO 19 – DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS 19
CAPÍTULO 20 – DAS DISPOSIÇÕES GERAIS 21
ANEXO I DOCUMENTOS INTEGRANTES DESTE EDITAL 23
ANEXO II ESPECIFICAÇÕES DOS GRUPOS E ITENS 24
ANEXO III MODELO DE PROPOSTA COMERCIAL 26
ANEXO IV MODELO DE DEMONSTRAÇÃO DE ATENDIMENTO AOS QUESITOS TÉCNICOS (PONTO A PONTO) 32

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

CAPÍTULO 01 – DA LEGISLAÇÃO APLICÁVEL

1.1. A licitação será regida pela Lei Federal nº 14.133/2021, pelo Decreto Estadual nº 10.086/2022, pelo Decreto Judiciário nº 269/2022, pela Lei Complementar Federal nº 123/2006, bem como as suas devidas alterações, e demais legislações complementares constantes no termo de referência.

CAPÍTULO 02 – DO OBJETO

2.1. Solução de TI consistente em serviços gerenciados de Segurança da Informação e Cibernética (MSS), com prestação contínua e sob demanda, aplicados ao ambiente tecnológico do Tribunal de Justiça do Estado do Paraná, pelo período de 36 (trinta e seis) meses prorrogável até o limite legal, conforme critérios, especificações e necessidades descritos no termo de referência e Anexo II, partes integrantes deste edital convocatório.

2.2. Havendo contradições entre a descrição dos bens constantes neste edital e seus anexos e aquela proposta pelo código CATMAT/CATSER, deve prevalecer a descrição do edital e seus anexos.

2.3. Deverão ser observados os requisitos da contratação, conforme disposto no capítulo 04 do termo de referência.

2.4. Deverão ser atendidos os modelos de execução do objeto estabelecidas no capítulo 05 do termo de referência.

2.5. Deverão ser atendidos os critérios de garantia e suporte estabelecidos no item 4.2 do termo de referência.

CAPÍTULO 03 – DO PREÇO MÁXIMO E DA DOTAÇÃO ORÇAMENTÁRIA

3.1. O preço máximo global deste certame está fixado em **R$ 29.035.777,53** (vinte e nove milhões, trinta e cinco mil, setecentos e setenta e sete reais e cinquenta e três centavos), conforme tabela contida no Anexo II.

3.2. A despesa decorrente da contratação ficará à conta da dotação orçamentária do Fundo de Reequipamento do Poder Judiciário - FUNREJUS, do exercício de 2026, estando o valor bloqueado por meio do(s) elemento(s):

Rubrica	Descrição
3.3.90.40.08	Despesa Corrente – Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica – Serviços Técnicos Profissionais de TIC

CAPÍTULO 04 – DA IMPUGNAÇÃO DO EDITAL E DA OBTENÇÃO DE ESCLARECIMENTOS

4.1. Qualquer pessoa é parte legítima para impugnar este edital por irregularidade na aplicação da Lei Federal nº 14.133/2021 e do Decreto Estadual nº 10.086/2022, ou para solicitar esclarecimentos e providências sobre os seus termos, no prazo de até 3 (três) dias úteis antes da data de abertura do certame.

4.2. As impugnações ou pedidos de esclarecimentos deverão ser formuladas por escrito e encaminhados ao endereço eletrônico licit@tjpr.jus.br, com a indicação da modalidade e número do certame, a razão social da empresa e seu telefone.

4.3. As impugnações e esclarecimentos serão respondidos no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame, e as respostas integrarão o edital e estarão disponíveis nos sites http://www.tjpr.jus.br/editais e https://www.gov.br/compras/.

4.3.1. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

CAPÍTULO 05 – DO CREDENCIAMENTO

5.1. O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores (SICAF), que permite a participação das interessadas em licitações realizadas por meio eletrônico.

5.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio https://www.gov.br/compras/, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil, em tempo hábil para participação neste certame.

5.3. O credenciamento junto ao provedor do sistema implica a responsabilidade da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a esta licitação.

5.4. A licitante se responsabiliza exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

5.5. Incumbirá à licitante acompanhar as operações no sistema eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Pregoeiro, pelo Agente de Contratação, pela comissão de contratação ou pelo sistema, ainda que ocorra sua desconexão.

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

CAPÍTULO 06 – DA PARTICIPAÇÃO

6.1. Poderão participar deste certame as interessadas cujo ramo de atividade seja compatível com o objeto da licitação e que atenderem a todas as exigências constantes deste edital e seus anexos.

6.2. É vedada a participação, direta ou indiretamente, de interessadas:

a) impedidas de licitar e contratar no âmbito do Estado do Paraná;

b) declaradas inidôneas para licitar ou contratar com a Administração Pública Federal, Estadual e Municipal, direta ou indireta, enquanto perdurar o motivo determinante da punição ou até que seja promovida a reabilitação;

c) que mantenham 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;

d) empresas controladoras, controladas ou coligadas, nos termos da Lei Federal nº 6.404/1976, concorrendo entre si;

e) 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;

f) que possuam em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação, em face da vedação estabelecida pela Resolução nº 229/16 do Conselho Nacional de Justiça;

g) reunidas em consórcio ou cooperativas, conforme justificativas apresentadas no termo de referência**.**

6.2.1. O impedimento de que tratam as letras “a” e “b” do item acima será também aplicado à 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 devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica da licitante.

6.3. Para participação no certame, a licitante deverá manifestar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do instrumento convocatório.

6.4. Para o Grupo 01 não serão assegurados os benefícios dos artigos 42 a 49 da Lei Complementar nº 123/2006 para as Microempresa e Empresas de Pequeno Porte que assim se identificarem no campo apropriado do sistema,

observado o disposto nos §§ 1º ao 3º, do art. 4º, da Lei nº 14.133/2021, vez que o valor do item ou grupo ultrapassa a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

6.5. Para o item 08, caso haja participação de microempresa (ME) ou empresa de pequeno porte (EPP), serão assegurados os benefícios da Lei Complementar nº 123/2006 para as pessoas jurídicas ou pessoas físicas que assim se identificarem no campo apropriado do sistema, sendo de responsabilidade exclusiva da licitante o seu correto enquadramento, observado o disposto nos §§ 1º ao 3º, do art. 4º, da Lei nº 14.133/2021.

6.5.1. A obtenção dos benefícios a que se refere o item acima, quando aplicáveis ao respectivo item/grupo, 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.

CAPÍTULO 07 – DO CADASTRAMENTO DAS PROPOSTAS INICIAIS

7.1. A proposta de preço inicial deverá ser cadastrada no sistema de compras eletrônicas no prazo previsto e de acordo com o critério de disputa estabelecido no edital.

7.1.1. Para fins de disputa, para o Grupo 01 será realizado o cadastramento de 7 (sete) itens no sistema ComprasGov, contemplando o valor total de cada subgrupo, todavia, a proposta apresentada deve levar em conta a totalidade de itens e demais obrigações previstas no termo de referência.

7.1.2. A licitante deverá dar oferta firme e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado.

7.1.3. A proposta registrada poderá ser alterada ou excluída até a data e hora definida no edital para abertura das propostas e, após este prazo, o sistema eletrônico não aceitará inclusão, alteração ou desistência da proposta.

7.2. Nos termos do Convênio ICMS nº 26/2003 – CONFAZ, quando se tratar de operação interna, as licitantes beneficiadas com a respectiva isenção fiscal devem apresentar as suas propostas e lances de com o valor líquido, ou seja, sem a carga tributária do ICMS.

7.2.1. Os estabelecimentos enquadrados no Regime Fiscal do Simples Nacional não estão abrangidos pelo disposto no item 7.2, devendo apresentar proposta com a carga tributária completa.

7.3. A licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

a) valor unitário e total do item;

b) descrição detalhada do objeto ou remissão ao item do edital que contenha as suas especificações.

c) marca, fabricante e modelo/versão, exceto quando se tratar de serviço.

7.4. Todas as especificações do objeto contidas na proposta vinculam a licitante e a contratada.

7.5. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na contratação, bem como todas as demais obrigações previstas no termo de referência e na minuta contratual.

7.6. Os valores ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade da licitante, não lhe assistindo o direito de pleitear qualquer alteração sob alegação de erro, omissão ou qualquer outro pretexto.

7.7. O prazo de validade da proposta não será inferior a 60 (sessenta) dias.

7.7.1. O prazo de validade da proposta inicial, previsto no item 7.7, terá início na data estabelecida para a abertura das propostas.

7.8. As propostas das licitantes devem respeitar os preços máximos estabelecidos neste edital, conforme artigo 27, XXI, da Constituição do Estado do Paraná.

7.9. No cadastramento da proposta inicial, a licitante declarará, em campo próprio do sistema, que:

a) está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

b) não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7°, XXXIII, da Constituição;

c) não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incs. III e IV, do art. 1º, e no inc. III, do art. 5º, da Constituição Federal;

d) cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.10. O fornecedor enquadrado como microempresa ou empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 3° da Lei Complementar nº 123/2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º, do art. 4º, da Lei nº 14.133/2021.

a) no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame, para aquele item;

b) nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de a licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123/2006, mesmo que microempresa ou empresa de pequeno porte.

7.11. A falsidade da declaração de que trata os itens 7.9 ou 7.10 sujeitará a licitante às sanções previstas na Lei nº 14.133/2021 e neste Edital.

7.12. Desde que disponibilizada a funcionalidade no sistema, a licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta, obedecendo às regras estabelecidas pelo próprio sistema.

7.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 7.12 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

CAPÍTULO 08 – DA ABERTURA DA SESSÃO E CLASSIFICAÇÃO DAS PROPOSTAS

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

8.2. Será desclassificada a proposta que identifique a licitante, com preço inexequível ou que não esteja em conformidade com os requisitos estabelecidos neste edital.

8.2.1. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

8.2.2. A classificação da proposta nesta fase não impede o seu julgamento definitivo em sentido contrário levado a efeito na fase de aceitação.

8.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

8.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro, Agente de Contratação ou comissão de contratação e as licitantes.

8.5. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão pública será automaticamente transferida para o primeiro dia útil subsequente, no horário estabelecido no preâmbulo deste edital, salvo comunicação do Pregoeiro, Agente de Contratação ou comissão de contratação em contrário.

CAPÍTULO 09 – DA FORMULAÇÃO DE LANCES

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

9.2. O lance deverá ser ofertado pelo valor total do item/grupo.

9.3. As licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no edital.

9.3.1. Cada licitante poderá ofertar lances para o Grupo 01 e o item 8, no entanto somente se sagrará vencedora de um deles.

9.3.2. Para efeito de adjudicação do objeto, o Grupo 01 e o item 8 deverão ser adjudicados a LICITANTES distintas que não tenham qualquer relação ou subordinação entre si, em razão da natureza dos serviços a serem contratados, que exige independência e autonomia entre os prestadores, de modo a garantir a integridade e a confiabilidade dos resultados pretendidos.

9.3.2.1. Cada LICITANTE poderá ofertar lances para o Grupo 01 e para o item 8, porém somente poderá ser vencedora de um deles. Assim, caso seja declarada vencedora do Grupo 01, será automaticamente desclassificada quanto ao item 8, que deverá ser analisado posteriormente ao Grupo 01.

9.3.3. A desclassificação decorrente da aplicação da regra prevista no item 9.3.2 não implicará a aplicação de sanções à LICITANTE desclassificada.

9.4. A licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ela ofertado e registrado pelo sistema.

9.5. O intervalo mínimo entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, será sobre o valor unitário do item conforme tabela abaixo:

Grupo	Item	Descrição	Intervalo mínimo entre lances
1	1	Projeto e implantação	R$ 5.000,00
	2	Serviços de Governança e Conformidade de Segurança	R$ 1.000,00
	3	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança	R$ 5.000,00
	4	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança	R$ 1.000,00
	5	Gestão de Vulnerabilidades e Testes de Segurança	R$ 1.000,00
	6	Gestão de Identidade	R$ 1.000,00
	7	Serviços Técnicos Especializados por Demanda	R$ 500,00
Item Avulso	8	PenTest	R$ 200,00

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

9.7. O modo de disputa adotado para a presente licitação será o **ABERTO.**

9.7.1. A fase de lances terá a duração de 10 (dez) minutos, sendo automaticamente prorrogada pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração inicialmente previsto.

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

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

9.7.4. Definida a melhor proposta, se a diferença em relação à classificada em segundo lugar for de pelo menos 5% (cinco por cento), poderá ser reiniciada a disputa aberta para a definição das demais colocações, sendo as licitantes convocadas para apresentarem lances intermediários.

9.8. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado por primeiro.

9.9. Durante todo o transcurso da sessão pública, as licitantes serão informadas em tempo real do valor de menor lance registrado, vedada a identificação da licitante.

9.10. Não poderá haver desistência dos lances ofertados, sujeitando-se a licitante desistente às penalidades constantes deste edital e da Lei nº 14.133/2021.

9.11. No caso de desconexão apenas do Pregoeiro ou Agente de Contratação, no decorrer da etapa competitiva, o sistema eletrônico permanecerá acessível às licitantes para a recepção dos lances. O Pregoeiro ou Agente de Contratação, quando possível, dará continuidade à sua atuação no certame, sem prejuízo dos atos realizados.

9.11.1. Quando a desconexão do sistema eletrônico para o Pregoeiro ou Agente de Contratação persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro ou Agente de Contratação aos participantes, no sítio eletrônico utilizado para divulgação.

9.12. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática do porte da entidade empresarial junto à Receita Federal. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123/2006.

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

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

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

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

9.13. 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.



9.13.1. Havendo empate entre propostas ou lances, o critério de desempate obedecerá a ordem prevista no art. 60 da Lei nº 14.133/2021 e no §3º do art. 91 do Decreto Estadual nº 10.086/2022.

CAPÍTULO 10 – DA NEGOCIAÇÃO

10.1. Após o encerramento da etapa de lances e depois de resolvidas as situações de empate ficto quando aplicáveis ao respectivo item/grupo**,** o Pregoeiro ou Agente de Contratação encaminhará contraproposta à arrematante para negociar condições mais vantajosas, observado o critério de julgamento e o valor máximo para a contratação, não se admitindo negociar condições diferentes das previstas neste edital.

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

10.3. Havendo apenas uma proposta, esta poderá ser aceita desde que atenda a todas as condições do edital, devendo o Pregoeiro ou Agente de Contratação negociar visando obtenção de melhor condição.

10.4. A arrematante que apresentar proposta acima do preço máximo ou inferior ao desconto mínimo definido para a contratação deverá readequá-la, sob pena de desclassificação.

10.5. Após a negociação, o Pregoeiro ou Agente de Contratação iniciará a fase de aceitação e julgamento da proposta.

CAPÍTULO 11 – DO ENVIO DA PROPOSTA RECOMPOSTA E DOCUMENTOS COMPLEMENTARES

11.1. O Pregoeiro ou Agente de Contratação solicitará à arrematante que envie, até as 12:00h (doze horas) do dia útil seguinte ao da convocação, a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares previstos neste edital.

11.1.1. É facultado ao Pregoeiro ou Agente de Contratação prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita pela arrematante antes de findo o prazo originalmente concedido.

11.1.2. Na recomposição final, os valores que compõem a proposta não poderão ultrapassar os valores máximos que estão fixados neste edital, bem como não poderão ser majorados os valores consignados na proposta inicial.

11.2. No mesmo prazo previsto acima, a arrematante deverá apresentar os seguintes documentos complementares:

a) proposta assinada, contendo obrigatoriamente todas as informações constantes do **modelo do Anexo III** (disponível para download no site https://www.tjpr.jus.br/editais);

a.1) na hipótese da proposta ser apresentada por procurador, deverá ser anexado o respectivo instrumento que demonstre os poderes para executar o ato;

a.2) a licitante deverá observar todas as disposições contidas no item 8.2 do termo de referência quando da elaboração de suas propostas de preços;

b) Demonstração do Resultado do Exercício - DRE atualizado, caso a microempresa, empresa de pequeno porte ou microempreendedor individual não seja optante do regime de tributação SIMPLES NACIONAL;

c) documentação de habilitação, prevista no Capítulo 13 do edital, que porventura não esteja disponível no SICAF ou encontre-se vencida;

d) declaração de que não se beneficiará, junto ao fabricante, de vantagens decorrentes do registro de oportunidade para parceiros comerciais ou prática semelhantes em detrimento dos demais concorrentes;

e) para os itens 3, 5 e 6 do grupo 1, declaração da licitante de que é fabricante ou parceira autorizada para comercializar e prestar os serviços previstos na contratação;

f) para o grupo 1, declaração de que atenderá integralmente aos seguintes itens, cuja documentação comprobatória deverá ser apresentada oportunamente como condição para a assinatura do contrato, sendo:

"Ao menos um SOC da CONTRATADA deverá possuir certificação ISO/IEC 27.001 vigente na contratação, emitida em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida";

g) planilha "ponto a ponto" (Anexo IV) de comprovação do atendimento da especificação das soluções informatizadas, indicando a documentação técnica (manual técnico, catálogo técnico, datasheet, folha de dados ou folha de especificações, artigo de conhecimento de suporte técnico e similares do fabricante), a página e/ou tópico onde se encontra cada informação, ou, alternativamente, imagens da console das soluções que comprovem o atendimento do requisito**.**

11.3. O Pregoeiro, Agente de Contratação ou comissão de contratação verificará se a licitante preenche os requisitos de participação, mediante consulta cadastral da empresa (Portal da Transparência do Governo Federal, TCU, SICAF, SIMPLES NACIONAL, GMS/PR, TCE/PR e Hermes/TJ-PR), bem como do sócio majoritário no cadastro nacional de condenações cíveis por ato de improbidade administrativa e inelegibilidade (CNIA/CNJ).

11.3.1. Será ainda consultada a situação da licitante no Cadastro Informativo Estadual – CADIN para verificar eventual impedimento de contratar e receber pagamentos.

11.3.2. Diante da suspeita de ocorrência impeditiva indireta prevista no art. 216 do Decreto Estadual nº 10.086/2022, o agente de contratação deverá suspender o processo licitatório, conforme procedimento do art. 217.

11.4. A licitante poderá se cadastrar junto ao sistema SEI-TJPR, por meio do endereço https://sei.tjpr.jus.br/externo, o qual será utilizado para assinatura de documentos relativos à contratação, futuras comunicações e ciência de outros atos decorrentes desta licitação.

11.4.1. Também serão considerados idôneos para todas as comunicações os meios indicados pela arrematante na sua proposta (telefone, endereço para correspondência e e-mail).

11.5. Dentro do prazo fixado no item 11.1 poderá ocorrer o saneamento de falhas, complementação de insuficiências ou correções de caráter formal relativos à proposta recomposta e documentos de habilitação. Excepcionalmente, o prazo poderá ser prorrogado a critério do Pregoeiro ou Agente de Contratação, mediante justificativa, em virtude da complexidade e/ou da quantidade de itens da licitação.

11.5.1. Em sede de diligência somente é possível a aceitação de novos documentos quando:

a) necessários para complementar informações acerca dos documentos já apresentados pela licitante e que se refiram a fato já existente à época da abertura do certame;

b) destinados à atualização de documentos vencidos após a data de recebimento das propostas.

11.6. Documentos ausentes ou fora de seu prazo de validade, quando disponíveis em sítios eletrônicos, poderão ser obtidos e anexados ao processo pela comissão de licitação.

11.7. O prazo de validade da proposta recomposta será o mesmo previsto no item 7.7 e terá início na data de sua apresentação.

11.8. A fim de subsidiar a Administração Pública quanto aos possíveis impactos tributários decorrentes da futura contratação, bem como para atender às exigências de planejamento orçamentário e eventual análise de reequilíbrio econômico-financeiro, a licitante vencedora deverá apresentar, no momento oportuno, tabela (modelo presente no Anexo III) contendo as seguintes informações relativas ao objeto contratado:

I – Enquadramento tributário da empresa contratada (inclusive quanto ao regime de apuração dos tributos incidentes);

II – Indicação das retenções tributárias aplicáveis aos bens e/ou serviços objeto da contratação, conforme legislação vigente.

11.8.1. O preenchimento incorreto ou incompleto da tabela mencionada não acarretará a desclassificação automática da licitante, devendo eventuais omissões ou inconsistências ser sanadas obrigatoriamente antes da homologação do certame, sob pena de inabilitação.

CAPÍTULO 12 – DO JULGAMENTO DA PROPOSTA

12.1. O critério de julgamento da presente licitação é o menor preço total/global por item/grupo.

12.1.1. Na hipótese de discrepância entre os montantes unitários e totais, para efeito de cotejo, prevalecerão os de menor valor.

12.2. No julgamento o Pregoeiro, Agente de Contratação ou comissão de contratação poderá, de forma fundamentada, sanar erros ou falhas que não alterem a substância da proposta, dos documentos e sua validade jurídica, para fins de classificação.

12.3. O Pregoeiro, Agente de Contratação ou comissão de contratação poderá realizar diligências para aferir a exequibilidade da proposta ou exigir da licitante que ela seja demonstrada.

12.4. O Pregoeiro, Agente de Contratação ou comissão de contratação poderá solicitar manifestação técnica de servidores pertencentes ao quadro de pessoal deste Tribunal de Justiça ou de pessoas físicas ou jurídicas estranhas a ele, para subsidiar suas decisões, indicando o dispositivo do edital de licitação objeto do questionamento e os documentos ou elementos sobre os quais recai a dúvida.

12.5. Será desclassificada a proposta:

a) formulada por quem esteja impedida de participar do certame;

b) que contenha qualquer oferta de vantagem não prevista neste edital, preços ou vantagens baseadas nas ofertas das demais licitantes;

c) que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração;

d) com preços superiores aos valores máximos que estão fixados no Anexo II, preços manifestamente inexequíveis ou que não tenham sua exequibilidade demonstrada, quando exigido pela Administração;

e) em desacordo com as especificações, prazos e condições fixadas neste edital;

f) que após diligências não forem corrigidas ou justificadas;

g) que contiver vício insanável.

12.6. No caso de desclassificação será examinada a proposta subsequente e assim sucessivamente até a apuração de uma que atenda a este edital, podendo o Pregoeiro ou Agente de Contratação negociar com a licitante para que sejam obtidas melhores condições.

12.7. Como condição de aceitação da proposta, o pregoeiro poderá, subsidiado pela equipe técnica, solicitar à licitante provisoriamente classificada em primeiro lugar a realização de Prova de Conceito (POC), quando restarem dúvidas quanto ao atendimento de um ou mais requisitos.

12.7.1. O pregoeiro irá agendar data e horário, com antecedência de até 10 (dez) dias úteis, para que a LICITANTE apresente os itens duvidosos através de Prova de Conceito (POC);

12.7.2. A Prova de conceito será realizada em ambiente preparado pela empresa classificada e apresentada de forma on-line, para que a LICITANTE demonstre a comprovação do atendimento dos requisitos enumerados, conforme as especificações exigidas no edital e seus anexos;

12.7.3. As despesas de preparação e apresentação da prova de conceito serão de responsabilidade da LICITANTE.

12.8. A não apresentação da prova de conceito no prazo sujeita a licitante desistente à desclassificação de sua proposta, sem prejuízo das penalidades constantes deste edital e da Lei nº 14.133/2021.

12.8.1. Excepcionalmente, dentro das hipóteses legais, poderá ser concedido prorrogação do prazo de entrega da prova de conceito para casos devidamente comprovados e justificados a serem analisados pelo setor técnico-operacional, desde que o pedido seja apresentado antes do escoamento do prazo.

CAPÍTULO 13 – DA HABILITAÇÃO

13.1. Para habilitação da licitante é necessária a documentação de:

a) habilitação jurídica;

b) regularidade fiscal, social e trabalhista;

c) qualificação econômico-financeira;

d) qualificação técnica.

13.2. Documentos relativos à **habilitação jurídica**:

a) cópia do contrato social ou instrumento equivalente (tais como estatuto social, requerimento de empresário ou certificado da condição de microempreendedor individual - CCMEI) com alterações e consolidação em vigor, acompanhada de documento comprobatório de seus administradores;

13.3. Documentos relativos às **habilitações fiscal, social e trabalhista**:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) do Ministério da Fazenda (comprovante emitido pela Receita Federal ou Certificado de Registro Cadastral – CRC, emitido pelo SICAF);

b) a inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade fiscal perante a Fazenda Municipal/Distrital do domicílio ou sede da arrematante;

d) prova de regularidade fiscal perante a Fazenda Estadual/Distrital do domicílio ou sede da arrematante;

e) prova de regularidade com a Fazenda Nacional, mediante a apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (SRFB) e Procuradoria Geral da Fazenda Nacional (PGFN);

f) prova de regularidade perante o Fundo de Garantia por Tempo de Serviço - FGTS, fornecido pela Caixa Econômica Federal – CEF;

g) prova de regularidade perante a Justiça do Trabalho;

h) demonstração de cumprimento do disposto no art. 7º, inc. XXXIII, da Constituição Federal.

13.4. Documentos relativos à **qualificação econômico-financeira**:

a) Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II); com data de expedição ou revalidação dos últimos 90 (noventa) dias anteriores à data da realização da licitação, caso o documento não consigne prazo de validade;

b) Balanço Patrimonial e Demonstração do Resultado do Exercício (DRE) dos dois últimos exercícios sociais, já exigíveis na data da apreciação da documentação entregue, assinados por Contabilista, devidamente registrado no Conselho Regional de Contabilidade e apresentados na forma da Lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados, quando encerrados há mais de 03 (três) meses da data de apresentação da proposta, tomando como base a variação, ocorrida no período, do ÍNDICE GERAL DE PREÇOS –DISPONIBILIDADE INTERNA –IGP-DI, publicado pela Fundação Getúlio Vargas –FGV ou de outro indicador que o venha substituir, sendo que, a memória de cálculo deverá ser apresentada com duas casas decimais, desprezando-se as demais;

b.1) As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

b.2) Todos os demonstrativos devem vir acompanhados dos termos de abertura e encerramento do livro diário, apresentados em cópia autenticada ou acompanhados dos originais para possibilitar a sua autenticação e registrados na Junta Comercial ou em outro órgão equivalente, com assinatura do contabilista responsável devidamente registrado no Conselho Regional de Contabilidade com CRC ativo e também a assinatura do titular da

empresa.

b.2.1) As empresas que utilizam a escrituração contábil digital poderão apresentar: balanço patrimonial e demonstração de resultado dos dois últimos exercícios sociais exigíveis, acompanhados dos respectivos termos de abertura e encerramento (relatório gerado pelo SPED) e recibos de entrega de livro digital na Receita Federal.

b.2.2) Para fins de aferição da exigibilidade das demonstrações contábeis referidas nos itens anteriores, observar-se-á o prazo previsto no art. 1.078 da Lei nº 10.406/2002 (Código Civil), correspondente aos quatro meses subsequentes ao término do exercício social, não se admitindo a prorrogação desse marco temporal em razão do prazo estabelecido para a transmissão da Escrituração Contábil Digital – ECD/SPED.

b.2.3) Na hipótese de as demonstrações contábeis exigidas ainda não se encontrarem chanceladas pelo órgão de registro competente, admitir-se-á, excepcionalmente, a apresentação do respectivo protocolo de entrega, desde que observado o prazo limite previsto no item b.2.2 acompanhado das correspondentes peças contábeis, devidamente assinadas por contabilista regularmente registrado no Conselho Regional de Contabilidade, o qual deverá declarar expressamente que os documentos apresentados correspondem integralmente aos documentos protocolizados perante o órgão de registro competente.

b.3) A comprovação de boa situação financeira da empresa, a que se refere a alínea “b”, será baseada na obtenção dos índices de Liquidez Geral (LG), Liquidez Corrente (LC) e de Solvência Geral (SG), maiores ou iguais a 1,0 (> ou = 1,0), resultante da aplicação das fórmulas:

$$LG = \frac{Ativo\ Circulante + Realizável\ a\ Longo\ Prazo}{Passivo\ Circulante + Passivo\ Não\ Circulante}$$

$$LC = \frac{Ativo\ Circulante}{Passivo\ Circulante}$$

$$SG = \frac{Ativo\ Total}{Passivo\ Circulante + Passivo\ Não\ Circulante}$$

b.4) Comprovação de Patrimônio Líquido não inferior 10% do valor estimado da contratação, na forma do § 4º do Art. 69 da Lei Federal nº 14.133/2021.

b.5) As empresas deverão apresentar o Capital Circulante Líquido - CCL (diferença entre o Ativo Circulante e o Passivo Circulante) não inferior a 8% (oito por cento) do valor máximo previsto para a contratação resultante da seguinte fórmula:

$$CCL = \frac{\text{Ativo Circulante} - \text{Passivo Circulante}}{\text{Valor Máximo da Contratação}}$$

c) Os índices previstos nos itens "b.3", "b.4" e "b.5" serão computadas com base nas demonstrações contábeis do último exercício social.

c.1) A ocorrência de algum equívoco na elaboração dos cálculos dos itens "b.3", "b.4" e "b.5", tendo a licitante fornecido dados que possibilitem a devida correção, não será motivo de inabilitação;

d) Com o objetivo de resguardar o Contratante dos riscos decorrentes do excesso de comprometimento econômico e financeiro por parte da contratada, os quais poderão interferir negativamente na boa execução contratual, a análise dos índices de comprovação da qualificação econômico-financeira de que tratam os itens "b.3", "b.4" e "b.5" considerará a soma dos valores das propostas finais para todos os lotes em que a licitante venha a se sagrar vencedora;

e) Justificativa das exigências de qualificação econômico-financeiras: os documentos, índices contábeis e demonstrativos patrimoniais solicitados para comprovação da qualificação econômico-financeira, representam, ressalvadas as hipóteses de desestabilização ocasionadas pela imprevisibilidade econômica do país, o mínimo

necessário para a aferição da boa situação financeira do licitante e do seu nível de organização contábil, bem como estão de acordo com o previsto no artigo 69 da Lei Federal nº 14.133/2021 e artigo 96 do Decreto Estadual nº 10.086/2022.

13.5. Documentos relativos à **qualificação técnica**:

13.5.1. A comprovação da qualificação técnica na habilitação da licitação será por meio de atestado(s) de capacidade técnico-operacional emitido(s) por pessoa jurídica de direito público ou privado em nome da LICITANTE, que comprove experiência que executou ou executa, de forma satisfatória, Serviços Gerenciados de Cibersegurança e/ou Segurança da Informação similares aos especificados no Termo de Referência.

13.5.2. Serão considerados compatíveis os atestados que comprovem a prestação de Serviços Gerenciados de Segurança (MSS), por pelo menos 12 (doze) meses, das seguintes parcelas de maior relevância:

Para o grupo 1:

1) Serviços prestados de governança e conformidade de segurança da informação ou cibersegurança, para instituição com no mínimo 2.000 (dois mil) usuários de tecnologia e contemplando no mínimo:

a) Elaboração de diagnósticos e avaliações de análise de Gap (situação e lacunas), maturidade e conformidade (com leis, normas e melhores práticas);

b) Elaboração e implantação de Plano de Continuidade de Negócios (PCN/BCP) e realização de Análise de Impacto nos Negócios (AIN/BIA);

c) Elaboração e revisão de políticas e normas, planos, procedimentos, indicadores e métricas de cibersegurança e/ou segurança da informação.

2) Serviços gerenciados prestados de monitoramento, detecção e resposta de eventos e incidentes de cibersegurança e/ou segurança da informação, em ambiente com no mínimo 3.000 (três mil) ativos ou 2.500 (dois mil e quinhentos) EPS (eventos por segundo), contemplando no mínimo:

a) Serviço de SOC (Security Operations Center) próprio da CONTRATADA;

b) Equipes de profissionais especializados em segurança da informação e cibersegurança, atuando em níveis 1, 2 e 3 de atendimento, operando em regime contínuo e ininterrupto 24x7x365;

c) Capacidade de inteligência de ameaças (Threat Intelligence), caçada contínua de ameaças (Threat Hunting) e gerenciamento de crises;

d) Operação de solução tecnológica especializada e atuação no gerenciamento, análise, triagem, automação e resposta de informações, eventos e incidentes de segurança.

3) Serviços de sustentação e operação de soluções de segurança contemplando no mínimo:

a) Solução de Next Generation Firewall Enterprise;

b) Soluções de Segurança de proteção de endpoint;

c) Solução de Gestão de Vulnerabilidade Tenable ou Qualys.

4) Serviços de gestão contínua de vulnerabilidades em ambientes com ao menos 1.000 (um mil) ativos e contemplando no mínimo:

a) Execução de varreduras de descoberta e conformidade em rede externa e interna para identificação, mapeamento e análise de vulnerabilidades em ativos corporativos de TIC;

b) Priorização de riscos cibernéticos de vulnerabilidades e ativos de TIC;

c) Operação de solução tecnológica especializada para gestão, varredura, avaliação e remediação de vulnerabilidades e de configuração segura, com análise e priorização do risco cibernético.

5) Serviços de gerenciamento de acesso privilegiado (PAM) em ambiente com no mínimo 25 (vinte e cinco) usuários administrativos ou 1.000 (um mil) ativos de TIC gerenciados.

Para o item 8:

1) Serviço de Teste de Invasão (Pentest), com no mínimo 150 horas, para exploração de vulnerabilidades de segurança da informação, que contenham pelo menos:

a) 1.000 (mil) usuários;

b) 1.000 (mil) ativos computacionais;

13.5.3. Será admitido o somatório de atestados para 50% do quantitativo exigido para a qualificação técnica, desde que demostrada a prestação do serviço de forma concomitante, o que pode ser comprovada por um único atestado ou por atestados distintos executados no mesmo período, demostrando a simultaneidade e a compatibilidade técnica entre os objetos. Além disso, para os outros 50% do quantitativo exigido para qualificação técnica deverá ser apresentado atestado único, não sendo admitido somatório.

13.5.4. Nos atestados deverão estar expressos, no mínimo, as seguintes informações:

a) Dados da empresa licitante: nome e CNPJ;

b) Dados da empresa cliente: nome e CNPJ;

c) Descrição dos serviços/fornecimento com dados que permitam o amplo entendimento dos trabalhos realizados e identifiquem a compatibilidade e semelhança com objeto da licitação;

d) Dados do emissor do atestado: nome e contato;

e) Data de emissão e assinatura do emissor.

13.5.5. O TRIBUNAL poderá promover diligências para dirimir quaisquer dúvidas, esclarecer ou complementar informações prestadas e aferir a veracidade das informações constantes nos atestados e documentos apresentados, incluindo visita presencial ao ambiente da CONTRATADA se julgar necessário, sob pena de desclassificação em caso de negação de diligências.

13.5.6. A licitante poderá disponibilizar todas as informações que entender necessárias à comprovação da legitimidade do atestado. Em caso de dúvidas, com relação ao conteúdo do atestado, poderá ser solicitado da licitante a apresentação de documentos como, por exemplo, contratos, notas de empenho ou notas fiscais etc.

13.5.7. Não será admitido atestado emitido por empresas pertencentes ao mesmo grupo econômico da proponente. Consideram-se pertencentes ao mesmo grupo econômico as entidades que embora tendo, cada uma delas, personalidades jurídicas próprias, mantiverem, entre si, direta ou indiretamente, relação de controle (art. 1.098 do Código Civil), ou estiverem sob o controle, direção ou administração, direta ou indireta, de outra pessoa física ou jurídica em comum.

13.5.8. A empresa licitante deverá apresentar comprovação ponto a ponto, contemplando os requisitos funcionais estabelecidos neste termo de referência, para cada uma das tecnologias e serviços exigidos e utilizados para a prestação do serviço contratado.

13.6. A habilitação da arrematante será verificada por consulta ao SICAF, bem como à documentação complementar que comprove o cumprimento dos requisitos previstos neste capítulo, a ser anexada ao sistema www.gov.br/compras, nos termos deste edital.

13.6.1. A licitante deverá confirmar se todos os documentos solicitados neste edital para verificação da habilitação estão inseridos e atualizados no sistema SICAF, caso contrário deverá providenciar a sua juntada.

13.7. Somente será considerada habilitada a arrematante que preencha os requisitos de habilitação na data da primeira sessão.

13.8. Nos casos de licitação fracassada, inclusive quanto ao respectivo grupo/item espelho, o Pregoeiro ou Agente de Contratação poderá conceder prazo de 08 (oito) dias úteis para a apresentação de novas propostas, corrigidas das causas que levaram à sua desclassificação/inabilitação.

CAPÍTULO 14 – DAS DISPOSIÇÕES GERAIS DA HABILITAÇÃO

14.1. Sob pena de inabilitação, os documentos deverão se referir ao CNPJ cadastrado no sistema www.gov.br/compras para a participação do certame.

14.1.1. Se a licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se a licitante for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica e no caso daqueles documentos que pela própria natureza forem emitidos somente em nome da matriz (FALÊNCIA – FEDERAL – FGTS – TRABALHISTA).

14.1.2. Caso a arrematante possua matriz e filiais na data da habilitação e participe da licitação com o CNPJ de uma delas, poderá executar o contrato e emitir as respectivas faturas com o CNPJ da outra, desde que comprove os requisitos de habilitação de ambas e indique em sua proposta o CNPJ (da matriz ou filial) que será utilizado para o faturamento, discriminando o item ou grupo respectivo, quando for o caso.

14.2. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a microempresa ou empresa de pequeno porte seja habilitada e declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

14.2.1. Na hipótese do item 14.2 será assegurado o prazo de 05 (cinco) dias úteis a partir do momento em que a arrematante for declarada vencedora, prorrogável por igual período, para a regularização da documentação, pagamento ou parcelamento do débito tributário ou fiscal, e obtenção das certidões negativas ou positivas com efeito de certidão negativa.

14.2.2. A não regularização da documentação implicará na decadência do direito à contratação, sem prejuízo das sanções previstas neste edital, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, ou revogar a licitação.

14.3. Toda a documentação apresentada deverá estar dentro do prazo de validade estabelecido pelo órgão expedidor e, quando omissa, será aceita por 90 (noventa) dias a partir da sua expedição.

14.4. Consideradas cumpridas todas as exigências do edital pela arrematante, o Pregoeiro, Agente de Contratação ou comissão de contratação a declarará vencedora e encaminhará o certame à autoridade superior para adjudicar o objeto e homologar a licitação.

14.4.1. A equipe de apoio ou comissão de licitação deverá solicitar à vencedora o cadastro obrigatório de usuário externo junto ao sistema SEI-TJPR, nos termos da normatização em vigor.

14.5. Ocorrendo a inabilitação, o Pregoeiro, Agente de Contratação ou comissão de contratação examinará a proposta subsequente na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital.

14.6. O Pregoeiro, Agente de Contratação ou comissão de contratação poderá sanar erros ou falhas que não alterem a substância da habilitação, dos documentos e sua validade jurídica, atribuindo-lhes validade e eficácia.

CAPÍTULO 15 – DOS RECURSOS

15.1. Qualquer licitante poderá manifestar a intenção de recorrer em campo próprio do sistema, de forma imediata após o término do julgamento das propostas e do ato de habilitação ou inabilitação, sob pena de preclusão.

15.1.1. Uma vez aceita a intenção de recurso será concedido o prazo de 3 (três) dias úteis para a apresentação das razões, ficando as demais licitantes, desde logo, intimadas para apresentarem as contrarrazões em igual prazo, que começará a contar do término do prazo da recorrente.

15.1.2. Será assegurada à licitante vista dos elementos indispensáveis à defesa de seus interesses, que deverá ser solicitada via e-mail para o endereço licit@tjpr.jus.br.

15.1.3. As razões recursais devem ser encaminhadas em campo próprio do sistema www.gov.br/compras.

15.2. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua 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, contado do recebimento dos autos.

15.3. O acolhimento do recurso implicará invalidação apenas de ato insuscetível de aproveitamento.

15.4. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório.

15.5. Não havendo recurso, o Pregoeiro, Agente de Contratação ou comissão de contratação encaminhará o procedimento à autoridade superior para adjudicar o objeto e homologar a licitação.

CAPÍTULO 16 – DA CONTRATAÇÃO

16.1. A contratação decorrente desta licitação será formalizada por termo de contrato, a ser assinado pela adjudicatária no prazo de 05 (cinco) dias úteis contados da data da convocação, podendo ser prorrogado uma vez por igual período a critério deste Tribunal, sob pena de decair do direito à contratação se não o fizer, sem prejuízo das sanções previstas neste edital.

16.2. Como condição para celebração do contrato a adjudicatária deverá:

a) manter as condições de habilitação;

b) não possuir fato impeditivo perante os cadastros do (Portal da Transparência do Governo Federal, TCU, SICAF, GMS/PR, TCE/PR, Hermes/TJ-PR e CNIA-CNJ);

c) não possuir registro no Cadastro Informativo Estadual – CADIN/PR, nos termos do art. 3º da Lei Estadual nº 18.466/2015, c/c. art. 7º do Decreto Estadual nº 1.933/2015.

16.3. A contratada deverá declarar ciência da Política de Relacionamento entre o Tribunal de Justiça do Estado Paraná e os seus Agentes com as Contratadas e as Potenciais Contratadas (Decreto Judiciário nº 62/2026 disponível em: https://www.tjpr.jus.br/legislacao-atos-normativos/-/atos/documento/4760362) e do Código de Ética e Conduta do Poder Judiciário do Estado do Paraná (disponível em: https://www.tjpr.jus.br/web/comissao-de-etica-e-de-conduta/codigo-de-etica-e-conduta).

16.4. Farão parte da contratação, independentemente de suas transcrições, as condições estabelecidas neste edital e na proposta da adjudicatária.

16.5. Em caso de recusa ou impossibilidade da adjudicatária em assinar o termo do contrato, aceitar ou retirar o instrumento equivalente, ou realizar os serviços, o Tribunal de Justiça adotará as providências cabíveis à imposição de sanção, bem como poderá convocar as licitantes remanescentes, respeitada a ordem de classificação, para, após comprovados os requisitos deste edital e feita a negociação, contratar com a Administração.

16.6. A correta emissão da nota fiscal é de responsabilidade da contratada e o faturamento deverá obedecer à legislação tributária que rege a matéria, devendo retratar a realidade da operação realizada e seus respectivos valores.

16.7. É obrigação da contratada manter, durante toda a execução do contrato, compatibilidade com as obrigações por ela assumidas e todas as condições de habilitação e qualificação exigidas na licitação.

16.8. Se houver previsão de garantia de execução, e sem prejuízo das disposições constantes do termo de referência, caso o adjudicatário opte pela modalidade seguro-garantia, a apólice deverá ser apresentada no prazo de até 1 (um) mês, contado da data de homologação da licitação, devendo ser comprovada a sua contratação previamente à assinatura do contrato, nos termos do §3º do art. 96 da Lei nº 14.133/2021.

CAPÍTULO 17 – DA EXECUÇÃO, FISCALIZAÇÃO, GESTÃO, RECEBIMENTO DO OBJETO E DO PAGAMENTO

17.1. As condições de entrega e/ou prestação dos serviços dar-se-ão segundo as regras previstas no termo de referência e na minuta contratual.

17.2. A fiscalização e a gestão da contratação dar-se-ão segundo as regras previstas no termo de referência e na minuta contratual.

17.3. O recebimento do objeto será feito em conformidade com o disposto no art. 140 da Lei Federal nº 14.133/2021 e as regras previstas no termo de referência e na minuta contratual.

17.4. O pagamento será efetuado de acordo com o prazo e as regras previstas no termo de referência e na minuta contratual.

17.4.1. A nota fiscal/fatura deve ser emitida com o CNPJ do Tribunal de Justiça do Estado do Paraná (77.821.841/0001-94).

17.4.2. O contratante efetuará a retenção da tributação pertinente, exceto quanto aos tributos PIS, COFINS e CSLL, em conformidade com a legislação aplicável, em especial a IN 01/2019-DTE/SEFA.

17.4.3. Como condição para o pagamento será consultada a situação da licitante no Cadastro Informativo Estadual – CADIN/PR, bem como a compatibilidade do CNAE com o objeto, para verificar eventuais impedimentos.

17.4.4. As condições para o reajustamento do contrato, inclusive o índice de reajustamento de preços, estão previstas na minuta contratual.

17.5. Ocorrendo atraso no pagamento, o contratante, se provocado, arcará com a correção do valor em atraso, estipulado com base na variação do Índice de Preços ao Consumidor Amplo – IPCA calculada *pro rata* para o período compreendido entre o término do prazo e a efetiva quitação do débito.

17.6. Os requerimentos ou manifestações da contratada, referentes à execução do objeto (por ex: alteração de marcas, prorrogação de prazos etc.), deverão ser devidamente motivados, instruídos com documentos hábeis e protocolizados antes do término do prazo de entrega, mediante formulário eletrônico disponível no endereço https://www.tjpr.jus.br/protocolo-admin.

17.6.1. O prazo de entrega do objeto ou da execução do serviço previsto originalmente não será suspenso, exceto quando autorizado na decisão da autoridade competente.

17.7. Durante a vigência do contrato, a contratada não poderá contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de dirigente do TJPR, nem de agente público que desempenhe função no processo de contratação ou atue na fiscalização ou gestão do contrato.

17.7.1. É vedado, ainda, participar da execução do contrato, direta ou indiretamente:

a) empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao Tribunal de Justiça do Estado do Paraná, em face da vedação estabelecida pela Resolução nº 09/05 do Conselho Nacional de Justiça;

b) quem 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.

17.7.2. É vedada a subcontratação:

I - de pessoa física:

a) que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do TJPR ou com agente público que desempenhe função no processo licitatório ou que atue na fiscalização ou gestão do contrato;

b) que seja cônjuge, companheiro(a) ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de dirigente do TJPR ou de agente público que desempenhe função no processo licitatório ou que atue na fiscalização ou na gestão do contrato.

II - de pessoa jurídica:

a) cujos dirigentes mantenham vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do TJPR ou com agente público que desempenhe função no processo licitatório ou que atue na fiscalização ou na gestão do contrato;

b) cujos dirigentes sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de dirigente do TJPR ou de agente público que desempenhe função no processo licitatório ou que atue na fiscalização ou na gestão do contrato.

CAPÍTULO 18 – DA LEI ANTICORRUPÇÃO

18.1. As licitantes e a contratada deverão atender às disposições contidas na Lei Federal nº 12.846/2013 – Lei Anticorrupção, motivo pelo qual, no decorrer da licitação e de todo o período contratual, conduzirão suas práticas comerciais de forma ética e em conformidade com os preceitos legais aplicáveis, não podendo dar, oferecer, pagar, prometer pagar, ou autorizar o pagamento, direta ou indiretamente, de qualquer valor, a quem quer que seja, com a finalidade de influenciar qualquer ato ou decisão, ou para assegurar qualquer vantagem indevida, ou direcionar negócios, e que violem o estabelecido na Lei Anticorrupção.

CAPÍTULO 19 – DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS

19.1. A licitante ou a contratada será responsabilizada administrativamente pelas seguintes infrações, conforme previsto na lei 14.133/2021, do Decreto Judiciário nº 269/2022 e do Decreto Estadual nº 10.086/2022:

I - dar causa à inexecução parcial do contrato;

II - dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

III - dar causa à inexecução total do contrato;

IV - deixar de entregar a documentação exigida para o certame;

V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

VI - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;

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

XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

XII - praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

19.1.1. Considera-se inexecução total do contrato:

I – recusa injustificada de cumprimento integral da obrigação contratualmente determinada;

II – recusa injustificada do adjudicatário em assinar ata de registro de preços, contrato ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela administração.

19.2. A licitante que incorrer nas infrações administrativas previstas no item 19.1. sujeitar-se-á às seguintes sanções:

I – advertência: exclusivamente pelas infrações administrativas do inciso I do item 19.1 e no caso de descumprimento, de pequena relevância, de obrigação legal ou infração à Lei quando não se justificar aplicação de sanção mais grave;

II - multa com relação a qualquer das infrações previstas no item 19.1, e será calculada na forma prevista neste edital e/ou no contrato;

III – impedimento: pelas infrações administrativas previstas nos incisos II a VII do item 19.1, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

IV – inidoneidade: pelas infrações administrativas previstas nos incisos VIII a XII do item 19.1, bem como pelas infrações administrativas previstas nos incisos II a VII do referido item que justifiquem a imposição de penalidade mais grave de impedimento, e impedirá o responsável de licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos;

19.3. Para fins de aplicação da advertência, considera-se pequena relevância o descumprimento de obrigações ou deveres instrumentais ou formais que não impactam objetivamente na execução do contrato, bem como não cause prejuízos à administração

19.4. A sanção de advertência, impedimento e inidoneidade poderão ser aplicadas cumulativamente com a multa.

19.5. As sanções de impedimento e inidoneidade serão aplicadas de modo independente em relação a cada infração diversa cometida.

19.5.1. Para o cômputo dessas sanções deverão ser observadas as demais regras dos arts. 224 a 225 do Decreto Estadual nº 10.086/2022.

19.6. A aplicação das sanções previstas nas alíneas do item 19.2. não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

19.7. Ficam estipuladas as seguintes multas, sem prejuízo de indenização suplementar em caso de perdas e danos decorrente da conduta:

19.7.1. Multa de 0,5% (zero vírgula cinco por cento) a 30% (trinta por cento), do valor total fixado no edital para os itens e/ou lotes objeto da proposta, para as infrações previstas nos incisos IV a VI e VIII a XII do item 19.1.

19.8. Caso a licitante incorra em uma das condutas elencadas no presente capítulo, será instaurado procedimento administrativo para apuração da irregularidade e a aplicação de sanções, no qual será assegurada a ampla defesa e o contraditório, observado o disposto no Decreto Judiciário nº 269/2022 e alterações posteriores.

19.9. Na aplicação das penalidades serão consideradas as circunstâncias do § 1º do art. 156 da Lei nº 14.133/2021, quais sejam:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - as circunstâncias agravantes ou atenuantes;

IV - os danos que dela provierem para a Administração Pública;

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

19.9.1. Deverão ser consideradas como agravantes e atenuantes as circunstâncias previstas nos incisos dos artigos 211 a 213 do Decreto Estadual nº 10.086/2022.

19.9.2. O cometimento de mais de uma infração em uma mesma licitação ou relação contratual sujeitará o infrator à sanção cabível para a mais grave entre elas, ou se iguais, somente uma delas, sopesando-se, em qualquer caso, as demais infrações como circunstância agravante, observando-se, ainda o previsto nos parágrafos do artigo 198 do Decreto Estadual 10.086/2022.

19.10. A personalidade jurídica poderá ser desconsiderada administrativamente, conforme previsto no art. 160 da Lei Federal nº 14.133/21, devendo ser observados os procedimentos previstos nos arts. 215 a 223 do Decreto Estadual nº 10.086/2022.

19.11. Após a regular tramitação do procedimento administrativo para apuração da irregularidade e a aplicação de sanções, havendo a aplicação da penalidade de multa, a empresa será notificada para o pagamento.

19.11.1. Transcorrido o prazo para o pagamento da multa, o Tribunal de Justiça poderá compensar o valor devido com qualquer crédito existente nesta ou em outra contratação.

19.11.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

19.12. Qualquer multa ou encargo imputado à empresa, não pago no prazo concedido pela Administração, será inscrito no CADIN Estadual e em Dívida Ativa do Estado e cobrado com base na Lei Federal nº 6.830/1980, sem prejuízo da correção monetária pelo IPCA ou outro índice que porventura venha a substituí-lo.

19.13. As disposições do Capítulo de Penalidades não excluem a responsabilização da licitante por eventuais atos lesivos previstos na Lei Federal nº 12.846/2013 e demais legislações, bem como a responsabilidade de indenização suplementar em caso de perdas e danos decorrente da conduta.

19.13.1. Nesses casos, os atos lesivos serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na lei nº 12.846/2013.

19.14. Quando a conduta da empresa acarretar a frustração do certame deverá ressarcir o Tribunal de Justiça no valor correspondente ao custo do processo de licitação, sem embargo de indenização suplementar caso o prejuízo exceda à referida quantia.

CAPÍTULO 20 – DAS DISPOSIÇÕES GERAIS

20.1. A licitante ou o interessado em participar da presente licitação consente e concorda com o tratamento e divulgação de seus dados pessoais para finalidade específica, conforme a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), a Lei nº 12.527/2011 e o princípio constitucional da publicidade.

20.2. É facultado ao Agente de Contratação, Pregoeiro, comissão de contratação e/ou à autoridade competente, em qualquer fase da licitação:

a) promover diligência destinada a esclarecer ou complementar a instrução do processo, inclusive com a juntada de novos documentos quando necessários para complementar informações acerca daqueles já apresentados pela licitante e que se refiram a fato pré-existente à abertura do certame, bem como aqueles destinados à atualização de documentos vencidos após a data de recebimento das propostas;

b) adotar medidas de saneamento destinadas a esclarecer informações, corrigir impropriedades na documentação de habilitação ou da proposta, ou complementar a instrução do processo, desde que não seja alterada a substância da proposta;

c) convocar licitantes para quaisquer esclarecimentos porventura necessários;

d) solicitar os documentos apresentados de forma eletrônica em original ou por cópia autenticada a qualquer momento, no prazo estabelecido.

20.3. A licitante que participar do certame fica plenamente ciente de que:

a) seu credenciamento como usuário externo perante este Tribunal no sistema SEI-TJPR poderá ser utilizado como meio válido para quaisquer comunicações, intimações e assinaturas decorrentes desta licitação, dos procedimentos administrativos e da contratação, bem como implicará em responsabilidade legal pelos atos praticados e presunção de capacidade e poderes conferidos para realização das transações inerentes aos documentos assinados;

b) é de sua exclusiva responsabilidade, como cadastrado e usuário externo do sistema SEI-TJPR, o sigilo da senha de acesso, não sendo admitida, em qualquer hipótese, alegação de uso indevido e que deverá comunicar imediatamente este Tribunal sobre a perda da senha ou a quebra de sigilo, para imediato bloqueio de acesso.

20.4. A homologação do julgamento caberá ao Presidente do Tribunal de Justiça, que poderá, em despacho circunstanciado e no interesse público, presentes os requisitos legais, revogar a licitação ou anulá-la na hipótese de ilegalidade, sem que caiba à licitante direito a indenização.

20.5. Na contagem dos prazos estabelecidos neste edital e no contrato exclui-se o dia do início e inclui-se o do vencimento, observadas as demais regras previstas no artigo 183 da Lei nº 14.133/2021.

20.5.1. Só iniciam e vencem os prazos em dia de expediente na Secretaria do Tribunal de Justiça, verificável através do endereço https://www.tjpr.jus.br/calendario.

20.6. Na hipótese de procedimento judicial, fica eleito o Foro Central da Comarca da Região Metropolitana de Curitiba para dirimir eventuais pendências oriundas da presente licitação, com renúncia de qualquer outro, por mais privilegiado que seja.

20.7. Eventual conflito na contratação poderá ser dirimido nos termos dos arts. 34 e 35 do Decreto Judiciário nº 269/2022.

20.8. Fica entendido que o presente edital e todos os seus anexos são complementares entre si, de modo que qualquer detalhe ou condição mencionado em um documento, mesmo que omitido em outro, será considerado especificado e válido para esta licitação.

Curitiba, 01 de outubro de 2026.

HERMES RIBEIRO DA FONSECA FILHO
Secretário de Contratações Institucionais

ANDRÉIA KARLA DORCE
Secretária de Tecnologia da Informação



TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ANEXO I
DOCUMENTOS INTEGRANTES DESTE EDITAL

Os seguintes documentos estão disponíveis para download no site https://www.tjpr.jus.br/editais:

- Estudo técnico preliminar (documento SEI!TJPR nº 12398584);
- Termo de referência (documento SEI!TJPR nº 13277407);
- Modelos de proposta e declarações;
- Mapa comparativo de preços (documento SEI!TJPR nº 13437116);
- Minuta contratual (documento SEI!TJPR nº 13542105).

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ANEXO II
ESPECIFICAÇÕES DOS GRUPOS E ITENS

GRUPO 01	PARTICIPAÇÃO GERAL				
	BENEFÍCIOS LC 123/2006		( ) SIM (X) NÃO		
ITEM	**QUANT.**	**UNIDADE DE MEDIDA**	**ESPECIFICAÇÕES**	**VALOR UNITÁRIO**	**VALOR TOTAL DO ITEM**
01	01	Unidade	Projeto e Implantação **CATSER:** 27022 **Item Sustentável:** NÃO	R$ 600.000,00	R$ 600.000,00
02	01	Unidade	Serviços de Governança e Conformidade de Segurança **CATSER:** 27340 **Item Sustentável:** NÃO	R$ 685.075,20	R$ 685.075,20
03	01	Unidade	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança **CATSER:** 27022 **Item Sustentável:** NÃO	R$ 17.279.117,13	R$ 17.279.117,13
04	01	Unidade	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança **CATSER:** 27022 **Item Sustentável:** NÃO	R$ 1.993.200,00	R$ 1.993.200,00
05	01	Unidade	Gestão de Vulnerabilidades e Testes de Segurança **CATSER:** 27022 **Item Sustentável:** NÃO	R$ 2.502.073,20	R$ 2.502.073,20
06	01	Unidade	Gestão de Identidade **CATSER:** 27022 **Item Sustentável:** NÃO	R$ 5.408.700,00	R$ 5.408.700,00
07	01	Unidade	Serviços Técnicos Especializados por Demanda **CATSER:** 27332 **Item Sustentável:** NÃO	R$ 429.372,00	R$ 429.372,00
VALOR GLOBAL *Considerar-se-á como global o somatório dos preços totais de cada item que compõe este grupo*				**R$ 28.897.537,53**	

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ITEM 08	PARTICIPAÇÃO GERAL			
	BENEFÍCIOS LC 123/2006	(X) SIM ( ) NÃO		
QUANT.	**UNIDADE DE MEDIDA**	**ESPECIFICAÇÕES**	**VALOR UNITÁRIO**	**VALOR TOTAL DO ITEM**
01	Unidade	Serviço de Teste de Invasão (Pentest) **CATSER:** 27022 **Item Sustentável:** NÃO	R$ 138.240,00	R$ 138.240,00

Observações:

1. Para fins de disputa, para o Grupo 01 será realizado o cadastramento de 7 (sete) itens no sistema ComprasGov, contemplando o valor total de cada subgrupo, todavia, a proposta apresentada deve levar em conta a totalidade de itens e demais obrigações previstas no termo de referência (Anexo I);
2. A proposta da empresa deve levar em conta todos os custos operacionais para o período de vigência da contratação, inclusive quanto à reoneração gradual prevista para o ano de 2026. Assim, a reoneração gradual, por ser previamente de conhecimento dos licitantes, não será fato ensejador de reequilíbrio econômico-financeiro.

Especificação detalhada do Grupo 01

	Item	Descrição	Qtde	Tipo	Valor Unitário	Valor Total
Grupo 01	1	Projeto e implantação	01	Unitário	R$ 600.000,00	R$ 600.000,00
	2	**Serviços de Governança e Conformidade de Segurança**				
	2.1	Diagnóstico de Maturidade de Segurança da Informação	03	Unitário	R$ 53.333,00	R$ 159.999,00
	2.2	Política de Segurança da Informação (PSI)	33	Mês	R$ 5.546,40	R$ 183.031,20
	2.3	Plano de Continuidade de Serviços Essenciais de TIC	33	Mês	R$ 5.166,00	R$ 170.478,00
	2.4	Plano de Resposta a Incidentes (PRI)	33	Mês	R$ 5.159,00	R$ 170.247,00
	3	**Monitoramento, Triagem, Tratamento e Resposta a Incidentes**				
	3.1	Serviço de Security Operations Center (SOC)	825.000	Ativos protegidos	R$ 19,78	R$ 16.318.500,00
	3.2	Proteção contra Riscos Digitais (Threat Intelligence)	33	Mês	R$ 24.678,61	R$ 814.394,13
	3.3	Serviço de Takedown	60	Takedown executado	R$ 2.437,05	R$ 146.223,00
	4	**Sustentação de Operações de Soluções e Resposta a Requisições de Segurança**				
	4.1	Solução de Firewall	198	Ativos protegidos	R$ 8.400,00	R$ 1.663.200,00
	4.2	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	660.000	Ativos protegidos	R$ 0,50	R$ 330.000,00
	5	**Gestão de Vulnerabilidades e Testes de Segurança**				
	5.1	Gerenciamento Contínuo de Vulnerabilidades	33	Mês	R$ 5.320,40	R$ 175.573,20
	5.2	Testes de Segurança Automatizados (BAS)	990	Baterias realizadas	R$ 2.350,00	R$ 2.326.500,00
	6	**Gestão de Identidade**				
	6.1	Gerenciamento de Acesso Privilegiado (PAM)	2.640	Usuários administrativos protegidos	R$ 2.048,75	R$ 5.408.700,00
	7	Serviços Técnicos Especializados por Demanda	1.200	Horas sob demanda	R$ 357,81	R$ 429.372,00

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ANEXO III
MODELO DE PROPOSTA COMERCIAL

PREGÃO ELETRÔNICO Nº 13/2026

CONTRATANTE

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ
CNPJ 77.821.841/0001-94

DADOS DA LICITANTE

Razão Social			
CNPJ		**CNPJ para faturamento** (matriz ou filial)	
Endereço			
CEP		**Telefone**	
E-mail *			

** O e-mail informado deverá ser o mesmo do cadastramento no SEI!*

DADOS DO REPRESENTANTE LEGAL/PROCURADOR

Nome *			
RG		**CPF**	

** Na hipótese de procurador, deverá ser anexado o respectivo instrumento que demonstre os poderes para executar o ato.*

DADOS PARA PAGAMENTO *

Inscrição Estadual		**Inscrição Municipal**	
CÓDIGO CNAE ** Atividade principal			
CÓDIGO CNAE Atividade do fornecimento			
Regime Tributário	**( ) SIMPLES ( ) LUCRO REAL ( ) LUCRO PRESUMIDO**	**Optante pelo SIMEI *****	**( ) SIM ( ) NÃO**

** A falta de preenchimento ou o preenchimento incorreto dos dados para pagamento não ocasionará a desclassificação da licitante, todavia podem inviabilizar o pagamento até as devidas correções.*

*** CNAE - Classificação Nacional de Atividades Econômicas. Disponível no cartão de CNPJ;*

**** SIMEI - Sistema de recolhimento em valores fixos mensais dos tributos abrangidos pelo Simples Nacional, devidos pelo Microempreendedor Individual (MEI);*

SOMENTE PARA ME OU EPP REGULAMENTADA PELA LEI COMPLEMENTAR Nº 123/06

Em atendimento ao art. 4º, §2º, da Lei Federal nº 14.133/2021, visando a obtenção dos benefícios da Lei Complementar nº 123/2006, declaro que:	**( )** **NÃO CELEBRAMOS** contratos com a Administração Pública no ano-calendário de realização da licitação cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.	**( )** **CELEBRAMOS** contratos com a Administração Pública no ano-calendário de realização da licitação cujos valores somados extrapolam a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.
SOMENTE PREENCHER EM CASO DE CONTRATAÇÃO DE SERVIÇO **O(s) serviço(s), no todo ou em parte pode(m) ser enquadrado(s) no seguinte Anexo da Lei Complementar nº 123/2006***	**ANEXO _____**	

** Algumas destas informações estão disponíveis no site http://www.sintegra.gov.br/*

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

GRUPO 01 — **PARTICIPAÇÃO GERAL**

	Item	Descrição	Qtde	Tipo	Valor Unitário	Valor Total
Grupo 01	1	Projeto e implantação	01	Unitário		
	2 Serviços de Governança e Conformidade de Segurança					
	2.1	Diagnóstico de Maturidade de Segurança da Informação	03	Unitário		
	2.2	Política de Segurança da Informação (PSI)	33	Mês		
	2.3	Plano de Continuidade de Serviços Essenciais de TIC	33	Mês		
	2.4	Plano de Resposta a Incidentes (PRI)	33	Mês		
	3 Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança					
	3.1	Serviço de Security Operations Center (SOC)	825.000	Ativos protegidos		
	3.2	Proteção contra Riscos Digitais (Threat Intelligence)	33	Mês		
	3.3	Serviço de Takedown	60	Takedown executado		
	4 Sustentação de Operações de Soluções e Resposta a Requisições de Segurança					
	4.1	Solução de Firewall	198	Ativos protegidos		
	4.2	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	660.000	Ativos protegidos		
	5 Gestão de Vulnerabilidades e Testes de Segurança					
	5.1	Gerenciamento Contínuo de Vulnerabilidades	33	Mês		
	5.2	Testes de Segurança Automatizados (BAS)	990	Baterias realizadas		
	6 Gestão de Identidade					
	6.1	Gerenciamento de Acesso Privilegiado (PAM)	2.640	Usuários administrativos protegidos		
	7	**Serviços Técnicos Especializados por Demanda**	1.200	Horas sob demanda		

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ITEM 08	PARTICIPAÇÃO GERAL			
	QUANT.	ESPECIFICAÇÕES	VALOR UNITÁRIO	VALOR TOTAL DO ITEM

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS								
ITEM	VALOR DO SERVIÇO R$ (A)	TRIBUTO	BENEFÍCIO FISCAL MARQUE COM "X" * (B)	BASE DE CÁLCULO R$ (C)	ALIQUOTA % ** (D)	VALOR A SER RETIDO R$ E = (C x D)	BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)
01	R$	IRPJ	SIM NÃO				
		CSLL	SIM NÃO				
		PIS/PASEP	SIM NÃO				
		COFINS	SIM NÃO				
		ICMS	SIM NÃO				
		ISS	SIM NÃO				
		INSS	SIM NÃO				

* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.

** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.

*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS								
ITEM	VALOR DO SERVIÇO R$ (A)	TRIBUTO	BENEFÍCIO FISCAL MARQUE COM "X" * (B)	BASE DE CÁLCULO R$ (C)	ALIQUOTA % ** (D)	VALOR A SER RETIDO R$ E = (C x D)	BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)
02	R$	IRPJ	SIM NÃO				
		CSLL	SIM NÃO				
		PIS/PASEP	SIM NÃO				
		COFINS	SIM NÃO				
		ICMS	SIM NÃO				
		ISS	SIM NÃO				
		INSS	SIM NÃO				

* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.

** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.

*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ITEM	VALOR DO SERVIÇO R$ (A)	TRIBUTO	BENEFÍCIO FISCAL MARQUE COM "X" * (B)				BASE DE CÁLCULO R$ (C)	ALIQUOTA % ** (D)	VALOR A SER RETIDO R$ E = (C x D)	BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)
03	R$	IRPJ		SIM		NÃO				
		CSLL		SIM		NÃO				
		PIS/PASEP		SIM		NÃO				
		COFINS		SIM		NÃO				
		ICMS		SIM		NÃO				
		ISS		SIM		NÃO				
		INSS		SIM		NÃO				

* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.

** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.

*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS

ITEM	VALOR DO SERVIÇO R$ (A)	TRIBUTO	BENEFÍCIO FISCAL MARQUE COM "X" * (B)				BASE DE CÁLCULO R$ (C)	ALIQUOTA % ** (D)	VALOR A SER RETIDO R$ E = (C x D)	BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)
04	R$	IRPJ		SIM		NÃO				
		CSLL		SIM		NÃO				
		PIS/PASEP		SIM		NÃO				
		COFINS		SIM		NÃO				
		ICMS		SIM		NÃO				
		ISS		SIM		NÃO				
		INSS		SIM		NÃO				

* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.

** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.

*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS

ITEM	VALOR DO SERVIÇO R$ (A)	TRIBUTO	BENEFÍCIO FISCAL MARQUE COM "X" * (B)				BASE DE CÁLCULO R$ (C)	ALIQUOTA % ** (D)	VALOR A SER RETIDO R$ E = (C x D)	BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)
05	R$	IRPJ		SIM		NÃO				
		CSLL		SIM		NÃO				
		PIS/PASEP		SIM		NÃO				
		COFINS		SIM		NÃO				
		ICMS		SIM		NÃO				

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

		ISS		SIM		NÃO				
		INSS		SIM		NÃO				

* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.

** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.

*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS										
ITEM	**VALOR DO SERVIÇO R$** (A)	**TRIBUTO**	**BENEFÍCIO FISCAL** **MARQUE COM "X" *** (B)				**BASE DE CÁLCULO R$** (C)	**ALIQUOTA % **** (D)	**VALOR A SER RETIDO R$** E = (C x D)	**BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)**
06	**R$**	**IRPJ**		**SIM**		**NÃO**				
		CSLL		**SIM**		**NÃO**				
		PIS/PASEP		**SIM**		**NÃO**				
		COFINS		**SIM**		**NÃO**				
		ICMS		**SIM**		**NÃO**				
		ISS		**SIM**		**NÃO**				
		INSS		**SIM**		**NÃO**				

* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.

** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.

*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS										
ITEM	**VALOR DO SERVIÇO R$** (A)	**TRIBUTO**	**BENEFÍCIO FISCAL** **MARQUE COM "X" *** (B)				**BASE DE CÁLCULO R$** (C)	**ALIQUOTA % **** (D)	**VALOR A SER RETIDO R$** E = (C x D)	**BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)**
07	**R$**	**IRPJ**		**SIM**		**NÃO**				
		CSLL		**SIM**		**NÃO**				
		PIS/PASEP		**SIM**		**NÃO**				
		COFINS		**SIM**		**NÃO**				
		ICMS		**SIM**		**NÃO**				
		ISS		**SIM**		**NÃO**				
		INSS		**SIM**		**NÃO**				

* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.

** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.

*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ENQUADRAMENTOS E RETENÇÕES TRIBUTÁRIAS								
ITEM	**VALOR DO SERVIÇO R$** (A)	**TRIBUTO**	**BENEFÍCIO FISCAL** **MARQUE COM "X" *** (B)				**BASE DE CÁLCULO R$** (C)	**ALIQUOTA % **** (D)	**VALOR A SER RETIDO R$** E = (C x D)	**BASE LEGAL DO BENEFÍCIO FISCAL *** (SE APLICÁVEL)**
08	**R$**	**IRPJ**		**SIM**		**NÃO**				
		CSLL		**SIM**		**NÃO**				
		PIS/PASEP		**SIM**		**NÃO**				
		COFINS		**SIM**		**NÃO**				
		ICMS		**SIM**		**NÃO**				
		ISS		**SIM**		**NÃO**				
		INSS		**SIM**		**NÃO**				
* No caso de serviços, **BENEFÍCIO FISCAL** abrange: isenção, imunidade e reduções da base de cálculo ou alíquota. Caso haja **BENEFÍCIO FISCAL** de algum tributo, marque **X** no campo **SIM**. Caso contrário, marque **X** no campo **NÃO**. Empresas inscritas no **SIMPLES NACIONAL**, **ENTIDADES SEM FINS LUCRATIVOS** e **ENTIDADES BENEFICENTES DE ASSISTÊNCIA SOCIAL** devem marcar **X** no campo **SIM** das linhas correspondentes ao IRPJ, CSLL, PIS/PASEP e COFINS.										
** Informe a alíquota do **IRPJ** que incidirá sobre a base de cálculo, conforme anexo I da IN RFB n° 1.234/2012. Informe as alíquotas do **ICMS**, **ISS**, e **INSS** que incidirão sobre a base de cálculo, conforme legislações aplicáveis.										
*** Detalhe artigo/inciso/etc da Lei ou Norma que proporciona BENEFÍCIO FISCAL para cada tributo, caso tenha marcado **X** no campo **SIM**. Deixe o campo em branco, caso tenha marcado **X** no campo **NÃO**.										

OBSERVAÇÕES:

- Os valores unitários, totais dos itens e o valor total para o grupo não poderão ser superiores aos fixados no Anexo II deste edital, sob pena de desclassificação da proposta;
- Os preços deverão ser cotados em moeda nacional, com no máximo duas casas decimais após a vírgula (R$ 0,00);
- O prazo de validade da presente proposta será de 60 (sessenta) dias a partir da data da sua apresentação;
- O preenchimento equivocado ou falta de preenchimento de alguma informação em relação à(s) tabela(s) de enquadramento e retenções tributárias não acarretará desclassificação automática da licitante, devendo ser saneado anteriormente à homologação do certame.

_____local_____, ___ de _____ de 20__.

_____
Assinatura

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

ANEXO IV
MODELO DE DEMONSTRAÇÃO DE ATENDIMENTO AOS QUESITOS TÉCNICOS (PONTO A PONTO)

Grupo 01

Item 2.4	Serviço de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança	Declaração/Comprovação (Documento, página, site etc.) de atendimento ao requisito.
2.4.1-1	O funcionamento do SOC deve ser em regime ininterrupto 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano (úteis e não úteis).	
2.4.1-2	A CONTRATADA deve atender uma das opções abaixo: a) possuir no mínimo 02 (dois) Centros de Operação de Segurança, sendo um em território nacional, redundantes e que devem estar em pleno funcionamento (infraestrutura física, lógica, equipe e processos) na contratação e durante toda a vigência do contrato, de modo que a indisponibilidade não afete a prestação dos serviços. O SOC principal e o redundante utilizados no serviço devem estar situados em regiões distintas, e estar no mínimo a 50 km (cinquenta quilômetros) de distância geodésica um do outro, como redundância geográfica para mitigar os riscos de interrupção dos serviços e de perda total dos dados em caso de desastres naturais, falhas de energia, entre outros eventos adversos. b) deve possuir 01 (um) Centro De Operações de Segurança (SOC) em território nacional, em pleno funcionamento (infraestrutura física, lógica, equipe e processos), na contratação e durante toda a vigência do contrato. A operação deve ser garantida de forma que a continuidade dos serviços não seja interrompida por tempestividades de qualquer natureza através da apresentação de um plano de continuidade.	
2.4.1-3	Deve possuir estrutura central para visualização dos painéis de monitoramento (video-wall) que permita que todos os profissionais visualizem informações e eventos relevantes simultaneamente.	
2.4.1-4	Deve utilizar sistema de gerenciamento de circuito fechado de televisão (CFTV), que viabilize o rastreamento de pessoas dentro do ambiente da CONTRATADA, e cujas imagens possam ser recuperadas, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias.	
2.4.1-5	Deve possuir controle de acesso físico seguro de funcionários, com pelo menos um dos seguintes fatores de autenticação: cartão de identificação magnético ou de proximidade, biometria de leitura de digital, face ou retina, e registro de entrada e saída de visitantes, com registro de entrada e saída de todas as pessoas mantido por pelo menos 90 (noventa) dias.	
2.4.1-6	Deve possuir perímetro físico equipado com sensor de intrusão e alarmes contra acesso indevido.	
2.4.1-7	Deve possuir estrutura de armazenamento de dados que permita a manutenção dos registros das requisições e dos incidentes relacionados aos serviços contratados por, no mínimo, o prazo do contrato.	



2.4.1-8	Deve possuir sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPS (Uninterruptible Power Supply), garantindo a transição entre o fornecimento normal da energia e o grupo gerador.	
2.4.1-9	Deve possuir componentes de segurança e plano de recuperação necessários para garantir a preservação dos dados em casos de incêndio e catástrofes.	
2.4.1-10	Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externa, desautorizadas.	
2.4.1-11	Deve possuir ambiente dedicado único e exclusivamente para laboratório, onde seja possível reproduzir os incidentes e problemas do TRIBUNAL, sem que haja impacto na operação dos SOCs e/ou do próprio TRIBUNAL.	
2.4.1-12	Deve garantir capacitação e treinamento inicial e contínuo dos profissionais que executam os serviços.	
2.4.1-13	Rever periodicamente as políticas e processos do SOC, a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL.	
2.4.3-1	Comprovar existência de equipe de tratamento e resposta a incidentes atuando em Nível 1 (atuação inicial), Nível 2 (atuação avançada) e Nível 3 (especialistas), organizada no mínimo em grupos distintos para: • Monitoramento e detecção de eventos, incidentes e ataques; • Caçada contínua a ameaças (Threat Hunting); • Inteligência de ameaças (Threat Intelligence); • Gestão de crises e investigação avançada de incidentes.	
2.4.3-2	Os times da CONTRATADA para segurança defensiva (Blue Team), ofensiva (Red Team) e mista (Purple Team) devem funcionar, interagir e atuar de maneira integrada, compartilhando conhecimento sobre táticas, técnicas e procedimentos de ataque, soluções para vulnerabilidades encontradas e outros, para que, por meio da atuação conjunta, aumente-se a efetividade da proteção do ambiente.	
2.4.3-3	A caçada contínua a ameaças (Threat Hunting) por meio de processos contínuos, estruturados e proativos, deve realizar, no mínimo, as seguintes atividades: • Definir hipóteses de possibilidades de ameaças e de como encontrá-las, elaboradas utilizando como referência vetores de ameaças novos e ativos e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, indicadores de comprometimento (IoC) de casos relevantes, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos (TTP), podendo ser utilizados Framework do MITRE ATT&CK, entre outros; • Planejar e realizar a coleta dos eventos dentro das plataformas relevantes de acordo com cada hipótese definida; • Avaliar a massa de eventos para buscar anomalias associadas à hipótese definida e registrar evidências encontradas; • Caso sejam encontrados eventos maliciosos e/ou incidentes, incluí-los no processo de tratamento e resposta a incidentes de segurança.	
2.4.3-4	O tratamento dos incidentes de segurança deve, alinhado com o Processo de Tratamento de Incidentes, realizar as seguintes ações:	

	• Efetuar a resposta, investigação e encerramento dos incidentes de segurança, incluindo o acionamento do seu Nível 2 e, nos casos de incidentes massivos e de severidade alta, seus especialistas de Nível 3; • Fazer a análise inicial dos incidentes confirmados e identificar os principais vetores de ataque e/ou exploração utilizados; • Classificar os incidentes em níveis de severidade, priorizar e escalar conforme o processo vigente; • Notificar o cliente, com os detalhes do incidente detectado e ativos de TIC envolvidos, de acordo com a severidade do incidente e a matriz de escalonamento no processo vigente; • Elaborar, executar e manter atualizados os roteiros de investigação e os playbooks de resposta a incidentes, com a devida aprovação final do cliente; • Automatizar playbooks por meio de ferramenta de orquestração e automação; • Prover a proposta de contenção, erradicação e recuperação, em articulação com as equipes do cliente, executar os procedimentos sob sua responsabilidade com a devida autorização do cliente e observado o processo de Gestão de Mudanças do cliente, e controlar as ações, notificações e escalonamento dos incidentes, de acordo com os roteiros de resposta pré-definidos; • Efetuar investigações relacionadas aos incidentes, com o objetivo de identificar a causa-raiz, coletar todas e quaisquer evidências e identificar os ativos de TIC afetados.	
2.4.3-5	Deve monitorar a atividade de ameaças e ocorrência de incidentes globais, através de feeds de inteligência de ameaças, identificados a partir de análises e pesquisas na DarkWeb e outras fontes de informação, de modo a antever eventuais ameaças e ataques ao TRIBUNAL e aprimorar os controles dos serviços contratados.	
2.4.4-1	Deve fornecer e adotar Solução Informatizada para Gerenciamento, Monitoramento, Detecção e Resposta de Informações, Eventos e Incidentes de Segurança e ataques, devendo ser projetada como uma plataforma completa e para atender funcionalidades de monitoramento, inspeção e análise, detecção contínua de ameaças e ataques, investigação e defesa cibernética	
2.4.4-2	Deve possuir arquitetura distribuída, com no mínimo as seguintes funcionalidades, módulos ou componentes nativamente integrados: • Gerenciamento de informações e eventos de segurança (Security Information and Event Management - SIEM) de nova geração; • Inteligência de ameaças (Threat Intelligence Platform - TIP); • Orquestração, automação e resposta (Security Orchestration, Automation and Response - SOAR); • Análise de comportamento de usuários e entidades (User and Entity Behavior Analytics - UEBA); • Detecção e Resposta de Rede (Network Detection and Response - NDR); • Malware Sandbox. Excepciona-se da obrigatoriedade de integração nativa, no parágrafo anterior, os componentes de Detecção e Resposta de Rede (NDR) e Malware Sandbox, os quais poderão ser providos por	



	meio de integração via APIs (Application Programming Interface) ou conectores específicos homologados pelo fabricante, desde que assegurada a total interoperabilidade e a capacidade de resposta orquestrada e automatizada dentro da plataforma principal.	
2.4.4-3	O gerenciamento de informações, eventos, alertas e incidentes deve possuir os seguintes recursos e capacidades: • Ingestão de dados, coleta de registros (logs) e telemetria e geração de metadados; • Indexação, agregação e enriquecimento dos metadados; • Retenção de dados e metadados e armazenamento de eventos e registros processados; • Correlacionamento, triagem e análises avançadas de eventos, alertas, detecção e tratamento de incidentes;	
2.4.4-4	Durante toda a vigência da contratação, não deve existir para a solução ofertada limitação quanto a quantidade de consultas de usuário nem de consultas programáticas (queries) às informações, quantidade de parses no tratamento de eventos, quantidade de conectores para ingestão, quantidade de envio de registros por ativo e quantidade de casos de uso.	
2.4.4-5	Ser extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período, preferencialmente adotando repositório em arquitetura “data lake”.	
2.4.4-6	Ter recursos de segregação lógica multilocação ("multitenancy") em uma arquitetura adequada para funcionar em ambiente multilocatário (“multitenant”).	
2.4.4-7	Ser dimensionada e licenciada para coletar, processar, correlacionar e armazenar eventos das fontes de dados do ambiente computacional on-premise e em nuvem do TRIBUNAL.	
2.4.4-8	Coletar, interpretar, normalizar e correlacionar eventos de segurança em tempo real, provenientes de logs de diferentes fontes do ambiente computacional do TRIBUNAL, com o objetivo de detectar incidentes e permitir a ação imediata da equipe de resposta a incidentes.	
2.4.4-9	Ser capaz de tratar, no mínimo, os seguintes formatos, protocolos e fontes: • Syslog, Simple Network Management Protocol (SNMP); • Microsoft Windows Event Log; • Logs em texto delimitado (como vírgula, tabulação, pipe); • Common Event Format - CEF, estruturado (ex: JSON, Regex etc.) ou não estruturado.	
2.4.4-10	Deve permitir a retenção do histórico de segurança da CONTRATADA, contemplando, minimamente, os seguintes dados: • Dados de eventos de segurança; • Dados das aplicações; • Dados dos sistemas operacionais; • Dados das nuvens públicas e privadas; • Dados do tráfego de rede; • Tráfego de registro (syslog).	
2.4.4-11	Ser capaz de coletar registros (logs) e informações de telemetria em serviços em nuvem pública de software (SaaS), plataforma (PaaS) e infraestrutura (IaaS), via integração por interfaces de programação (APIs),	



	protocolos e agentes que sejam providos e homologados no mínimo pelos seguintes provedores: • Amazon Web Services (AWS); • Google Cloud Platform (GCP); • Microsoft Azure, Oracle Cloud.	
2.4.4-12	Ser capaz de inspecionar registros de plataformas de colaboração corporativa como Google Workspace e Microsoft/Office 365.	
2.4.4-13	Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) e soluções de gestão de identidade.	
2.4.4-14	Possuir API restful para integração com vários serviços para ingestão de registros, telemetria e tráfego para detecção e resposta a eventos de segurança.	
2.4.4-15	Prover mecanismo de coleta de logs de dispositivos e fontes não suportados nativamente, por meio de personalização de coletores.	
2.4.4-16	Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta.	
2.4.4-17	Possuir mecanismos de compressão e controle de fluxo para a transmissão de dados entre os coletores e os servidores de gerenciamento, através de um dos componentes da solução (aplicação, sistema operacional, etc).	
2.4.4-18	Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume de eventos.	
2.4.4-19	Armazenar os alertas, incidentes e os eventos, inclusive os normalizados, de forma indexada.	
2.4.4-20	Toda a comunicação entre os componentes deve ser criptografada.	
2.4.4-21	Possuir política de retenção configurável para o tempo de armazenamento de eventos em formato bruto (raw), preservando evidências para fins de conformidade e eventuais ações forenses, com retenção de dados brutos pelo período mínimo de 30 (trinta) dias.	
2.4.4-22	Reter os dados processados e metadados de eventos, como alertas e registro de incidentes gerados, em registros no banco de dados e/ou data lake da solução pelo período mínimo de 12 (doze) meses, meses, salvo para consultas e pesquisas on-line, devendo, no mínimo, os últimos 30 (trinta) dias de registros serem armazenados a quente (hot-storage).	
2.4.4-23	Proteger os registros contra perdas, destruição, falsificação, acesso não autorizado e liberação não autorizada.	
2.4.4-24	Permitir o expurgo dos dados de forma automática, com a personalização do prazo de expurgo, sendo que somente será permitida a exclusão de eventos conforme a política de retenção de dados definida, ou seja, todos os eventos mais antigos que extrapolem o tempo de retenção definido.	
2.4.4-25	Permitir a correlação de eventos, devidamente estruturados em metadados.	
2.4.4-26	Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas também deve ser capaz de criar novos analisadores personalizados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis.	



2.4.4-27	Permitir filtrar e selecionar os eventos que serão inseridos na solução e a criação e alteração de filtros.	
2.4.4-28	Tratar eventos e alertas em um fluxo de refinamento, através de categorização e priorização, análise crítica, investigação, enriquecimento de informações e análises, inteligência de ameaças (Threat Intelligence) incluindo fontes estratégicas (relatórios, bases de conhecimento, feeds, fóruns e comunidades abertas, da Deep Web e da Dark Web etc.), táticas (correlação com táticas, técnicas e procedimentos - TTPs) e operacionais (correlação com indicadores de comprometimento - IOCs), e validação, identificando atividades anômalas e, dentre essas, candidatos a incidentes.	
2.4.4-29	Deve realizar análise comportamental de usuários e entidades (User and Entity Behavioral Analysis - UEBA) com aprendizado de máquina para detectar ameaças.	
2.4.4-30	Deve ser capaz de detectar padrões de ataques, através da elaboração de baseline comportamental dos usuários e entidades.	
2.4.4-31	Deve possuir técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal.	
2.4.4-32	Deve possuir a capacidade de identificar anomalias nos comportamentos individuais dos usuários e entidades: • Horário atípico do acesso; • Número atípico de sessões de uso nos sistemas operacionais; • Volume de conexões atípico; • Volume de transferências de dados atípico; • Localização geográfica atípica da origem do acesso; • Endereço IP de origem atípico do acesso; • Acesso atípico a dados armazenados; • Criação e uso de processos (executáveis em memória) atípicos pelo usuário/entidade; • Mudança na postura de risco do usuário/entidade.	
2.4.4-33	Deve enriquecer os eventos em tempo real com o contexto do usuário e da entidade. Os dados enriquecidos devem fornecer atributos de contexto que podem ser usados para a elaboração de perfis de comportamento, comparações entre pares, pesquisas e investigações.	
2.4.4-34	Implementar regras avançadas que conectem eventos sem correlação direta e gerem incidentes caso seja constatado algum desvio.	
2.4.4-35	Possuir capacidade de contextualização, utilizando dados de diferentes origens (servidores, aplicações etc.) em uma única console, otimizando o processo de análise e resposta a incidentes.	
2.4.4-36	Agregar eventos semelhantes que ocorrerem dentro de um limite de tempo ou quantidade de eventos específicos.	
2.4.4-37	Possuir identificação autônoma de táticas, técnicas e procedimentos (TTPs) mapeando automaticamente com o framework MITRE ATT&CK.	
2.4.4-38	Deve incluir capacidades de integração nativa com ferramentas de proteção, detecção e resposta de endpoints (Endpoint Protection Platforms - EPP e Endpoint Detection and Response - EDR), incluindo obrigatoriamente a atual do TRIBUNAL - Microsoft Defender.	



2.4.4-39	Deve permitir modelagem de ameaças com a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco.	
2.4.4-40	Deve possuir tecnologia para análise automatizada de artefatos maliciosos (“malware sandbox”) que minimamente contemple as funcionalidades a seguir: • Analisar indicadores comportamentais de um artefato; • Realizar análise estatística e dinâmica para validar se o artefato é malicioso ou não; • Suportar a análise de artefatos BAT, CHM, DLL, EXE, ISO, HTA, JAR, JS, JSE, LNK, MSI, MHTML, documentos do Microsoft Office, PE32, PDF, VBE, VBS, WSF, XML, ZIP.	
2.4.4-41	Permitir a caçada rápida de ameaças por meio da pesquisa em linguagem natural.	
2.4.4-42	Deve ser eficaz na detecção de ameaças e ataques de Ransomware.	
2.4.4-43	Deve ser capaz de detectar no mínimo as seguintes ameaças de identidade: • Password spray; • Brute force; • Varredura de credenciais; • Golden ticket; • Pass-the-hash; • Atividade não usual/atípica de usuário; • Elevação de privilégios; • Movimentação lateral.	
2.4.4-44	Apresentar as informações sobre os eventos que compõem um alerta ou incidente identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente.	
2.4.4-45	Possuir um sistema de alertas personalizável pelo administrador da solução, com a possibilidade de geração de alertas via dashboard automatizados ou e-mail quando um incidente for detectado.	
2.4.4-46	Permitir a criação e o gerenciamento de detecção de ameaças e conformidade na forma de regras, análises, relatórios e dashboards.	
2.4.4-47	Deve suportar controle de acesso baseado em função (RBAC) granular com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações.	
2.4.4-48	Possuir workflow automatizado para a resposta e gerenciamento de incidentes, de modo que ações de criação, alteração, escalonamento, documentação e fechamento de incidentes possam ser realizadas automaticamente pela solução.	
2.4.4-49	Prover acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesenvolvimento.	
2.4.4-50	Possuir funcionalidades de atualização, gerenciamento e configuração centralizadas de todos os agentes ou conectores distribuídos da solução.	
2.4.4-51	Permitir a categorização manual de eventos inéditos não categorizados por padrão e sua aplicação em eventos futuros de mesma natureza.	



2.4.4-52	Permitir pesquisas no histórico de eventos, fornecendo capacidade de visualizar os detalhes dos eventos (drill down), inclusive no formato bruto, quando aplicável, para análise forense e investigação de incidentes.	
2.4.4-53	A partir de um evento ou conjunto de eventos, apresentar seus relacionamentos de forma gráfica e possibilitar fazer drill down para efetiva investigação e identificação de causa raiz.	
2.4.4-54	Gerenciamento, análise, orquestração e automação de políticas, posturas, casos de uso, playbooks e integrações, com capacidade de resposta autônoma e aplicação próxima a tempo real, com componente de Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation and Response - SOAR), totalmente e nativamente integrado à solução, com o objetivo de automatizar os processos e fluxos de trabalho, a execução de atividades repetitivas ou de difícil execução e a orquestração das diversas ferramentas de segurança, com necessidade mínima de atuação humana.	
2.4.4-55	Deve possuir integração nativa com os diversos ativos e recursos de infraestrutura e segurança de TIC e capacidade de integrar, consolidar, agregar e correlacionar também todas as informações oriundas de outras fontes de telemetria disponíveis.	
2.4.4-56	Deve prover plataforma para gerenciamento e documentação de eventos/incidentes/casos de uso de ponta a ponta, automação de resposta a incidentes, investigação, automação de playbooks e repositório único de evidências.	
2.4.4-57	Não deve ter restrições com limitações de licença sobre o número de casos, número de playbooks criados ou número de ações realizadas pelos usuários do sistema.	
2.4.4-58	O recurso de gerenciamento de incidentes deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até a sua resolução e prevenção, gerenciando eficazmente incidentes.	
2.4.4-59	A CONTRATADA deverá promover a automação de processos e fluxos de trabalho em solução interativa, prática e de fácil implementação, sem a necessidade de customização ou alteração do código-fonte.	
2.4.4-60	Os Dashboards (painéis), gráficos e relatórios, devem: • Fornecer dashboards e relatórios pré-configurados e permitir a criação de dashboards e relatórios personalizados de forma flexível, ágil e intuitiva, incluindo gráficos como tipo pizza, linha, colunas, barras e tabelas dinâmicas, contemplando as diversas necessidades de visão gerencial; • Possuir dashboards de monitoramento em tempo real e de dados históricos; • Permitir a emissão de relatórios de forma tempestiva ou agendada, permitindo configurar o envio automático e agendado para grupos de usuários ou usuários específicos; • Permitir a sobreposição e o cruzamento de informações, e agrupamentos por critérios comuns; • Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards, ajustando o layout e conteúdo do painel de acordo com suas necessidades.	
2.4.4-61	Permitir que a partir de qualquer gráfico de gestão, contido em painéis e dashboards, o usuário possa, de forma gráfica e interativa:	



	• Clicar e listar os registros relacionados com os dados contidos no gráfico (drill down); • Realizar alterações dinâmicas de atributos, como a alteração de eixos, título, legenda, escala, rótulos de dados, tamanho; • Permitir o gerenciamento de permissões por usuários e grupos para acesso aos dashboards e relatórios e para compartilhamento; • Permitir a geração de relatórios, impressão e exportação para arquivos em formatos como .csv e .pdf.	
2.4.4-62	Permitir integração com a Solução Informatizada para Gestão de Vulnerabilidades, adquirida pelo TRIBUNAL.	
2.4.4-63	Quanto ao mecanismo de detecção e resposta na rede (NDR): • Ser capaz de analisar o tráfego TCP/UDP na rede da CONTRATANTE para detectar comportamentos e possíveis ameaças, gerando eventos de alerta de acordo com o tipo de tráfego; • Ser capaz de produzir e coletar informações de telemetria de tráfego de rede, tomando como base no mínimo as conexões de rede principais do data center do TRIBUNAL; • Suportar a análise de no mínimo 08 (oito) Gbps de tráfego total, incluindo tráfego criptografado, devendo ser fornecidos equipamentos capazes de realizar espelhamento de tráfego (seja incluso em Appliance ou por meio de derivação de rede - Network Tap) com no mínimo duas interfaces fibra óptica de 10 (dez) Gbps cada, com especificações de SFP a serem oportunamente fornecidas pelo TRIBUNAL; • Ser capaz de funcionar em modo de monitoramento, sem bloquear comunicações maliciosas de entrada ou saída; • Ser capaz de inspecionar cada pacote individualmente e detectar e extrair adequadamente o protocolo e serviço, contornando de forma confiável eventuais medidas de evasão.	
2.4.4-64	Ter a capacidade de identificar ameaças no tráfego de rede e realizar o monitoramento proativo de forma automatizada o tráfego passante na rede da CONTRATANTE, contemplando os seguintes critérios: • Utilização da largura de banda; • Tentativas de invasão e varreduras de IPs e portas; • Autenticações recusadas ou com falhas; • Análise de arquivos benignos e maliciosos e suas respectivas categorias; • Ataques de negação de serviço; • Conexões de comando e controle presentes, internamente ou para a Internet; • Dispositivos que representam o maior risco; • Tempos de resposta, tráfego de entrada e saída (inbytes/outbytes); • Aplicações que consomem mais recursos de rede; • Análise de DNS (tempos de resposta, comunicação, time-out, erros e desempenho); • Identificação de aplicações da Camada 7; • Principais eventos críticos de segurança; • Monitoramento de certificado SSL; • Identificação da versão do Windows;	



	• Ataques de adivinhação de credenciais (força bruta, password spraying).	
2.4.4-65	Suportar o protocolo HTTP/2.	
2.4.4-66	Ser capaz de detectar tráfego de rede potencialmente malicioso, como ransomware, movimentação lateral, consultas e conexões de comando e controle (C&C), mineração de criptomoedas (crypojacking), Mimikatz e outros, incluindo as que se aproveitam do tráfego RPC e SMB.	
2.4.4-67	Ser capaz de exportar de forma inteligente arquivos duplicados e limitar o comprimento das exportações, reduzindo a carga nas estruturas de análise de arquivos.	
2.4.4-68	Ser capaz de ativar monitoramento personalizado e prover extensibilidade de detecção por meio de padrões abertos.	
2.4.4-69	Ser capaz de identificar táticas e técnicas adversárias segundo o modelo MITRE ATT&CK.	
2.4.5-1	A CONTRATADA deve realizar Proteção contra Riscos Digitais (Threat Intelligence) com o monitoramento da marca e da reputação institucional na Internet, na Deep Web e na Dark Web, incluindo redes sociais, serviços de comunicação, repositórios de informação e lojas de aplicativos, identificando fraudes e golpes, conteúdo malicioso, vazamentos de dados e ameaças externas globais e com foco em Brasil, Governo e Judiciário, e providenciar Takedown em nome do TRIBUNAL mediante procuração e autorização.	
2.4.5-2	As fontes de monitoramento devem incluir, no mínimo: • Sites e serviços na internet (aberta ou superficial), na deep web (internet profunda) e na dark web (internet obscura); • Registros de domínios nacionais e internacionais, incluindo TLDs e gTLDs; • Perfis e comunidades em redes sociais e plataformas de mídias sociais, contemplando no mínimo Facebook, Instagram, Twitter, YouTube e LinkedIn, e desejável também Flickr; • Grupos, canais e comunidades em serviços de comunicação por mensagens e fóruns, contemplando no mínimo Telegram e Discord, e desejável também WhatsApp; • Repositórios e serviços de conteúdo e informação de grande abrangência, como Github e Gitlab; • Lojas de aplicativos (catálogo ou repositório de distribuição de software instalável para determinada plataforma de sistema operacional), contemplando no mínimo Google Play (Android), Apple App Store (iOS/iPadOS) e Microsoft Store (Windows), e desejável também Samsung Galaxy Store (Android) e F-Droid (Android).	
2.4.5-3	O monitoramento deve abranger conteúdo e informações em texto, mídias de imagem, áudio e vídeo, incluindo o reconhecimento e análise de texto em arquivos e bases de dados, e desejável também em imagens (Optical Character Recognition - OCR).	
2.4.5-4	O serviço deve identificar, no mínimo: • Fraudes, phishing e outros tipos de golpes, conteúdo malicioso e ameaças relacionadas; • Réplicas, conteúdos ilegítimos, abusos e violações aos serviços utilizando nome, marca e/ou logomarca institucionais do TRIBUNAL;	



	• Typosquatting (variações de nome, permutações de caracteres e outras variantes visando erros comuns de digitação) e variações ilegítimas ou maliciosas de domínio, certificado SSL/TLS, marca institucional e outros nomes objeto do monitoramento; • Vazamento de dados, credenciais e informações de segurança e institucionais sensíveis e confidenciais; • Violação de direitos de uso do TRIBUNAL ou a tentativa de burlar os meios de proteção desses direitos.	
2.4.5-5	Em caso de suspeita ou identificação de ocorrências monitoradas, a CONTRATADA deve realizar no mínimo as seguintes atividades: • Registrar e gerenciar o incidente em todo o seu ciclo de vida; • Notificar e emitir alertas, bem como confirmar eventuais suspeitas junto ao TRIBUNAL; • Comunicar a obrigação de Takedown (desativação administrativa e retirada do ar) do objeto do incidente aos administradores do seu anfitrião (host); • Acompanhar o andamento e efetivação do Takedown; • Analisar e investigar a rastreabilidade da ocorrência, visando identificar informações relevantes como autoria, linha do tempo, técnicas, meios e caminho de obtenção, exfiltração, propagação e veiculação; • Elaborar e apresentar relatórios de andamento e análise; • Monitorar a possibilidade de reincidência da ocorrência por, no mínimo, 30 (trinta) dias corridos a partir da efetivação do Takedown; • Tomar providências cabíveis em seu âmbito de atuação visando garantir a eficácia do Takedown, incluindo reiterar e obter esclarecimentos junto aos administradores do anfitrião; • Subsidiar informações ao TRIBUNAL para a criação e melhoria de controles de segurança aplicáveis para evitar ocorrências similares futuras.	
Item 2.6	GESTÃO DE VULNERABILIDADES E TESTES DE SEGURANÇA	
2.6.2.1-1	Fornecimento e sustentação de solução informatizada de Simulação de violações e ataques (Breach and Attack Simulation - BAS), composta por agentes (softwares) ou atores (simuladores virtuais), conforme exigências descritas neste documento.	
2.6.2.1-2	Os itens que compõem a Solução de BAS e seu sistema de gerenciamento devem ser produzidos pelo mesmo fabricante.	
2.6.2.1-3	Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado.	
2.6.2.1-4	A solução deve contemplar a versão de software e/ou firmware mais estável e recomendado pelo fabricante.	
2.6.2.1-5	O fabricante deve possuir rede de inteligência (threat inteligence) própria da solução para atualização constante de ameaças (threat feed) de forma automática.	
2.6.2.1-6	Deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno,	



	e endpoint, com comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, cobrindo no mínimo o sistema operacional Microsoft Windows.	
2.6.2.1-7	As simulações devem garantir ambiente controlado e sem impacto nocivo real, ou seja, não deverá trazer qualquer risco real de infectar a rede do TRIBUNAL em suas atividades.	
2.6.2.1-8	Os resultados devem validar e indicar controles de prevenção e proteção ineficazes e/ou suplantados, vulnerabilidades exploradas, caminhos de ataque e TTPs (táticas, técnicas e procedimentos) envolvidos de acordo com o framework MITRE ATT&CK.	
2.6.2.1-9	Permitir o gerenciamento centralizado da ferramenta, por meio de interface gráfica (GUI), nos formatos web segura (https) ou em formato de aplicativo cliente compatível com Windows 10 e superior, podendo ser em nuvem (cloud), appliance virtual ou por meio da própria solução.	
2.6.2.1-10	A solução deve possuir agentes (softwares) que possam ser instalados em máquinas, ou em ambientes virtuais (servidores), confeccionadas para simulação de ataques, ou apresentar atores (simuladores) virtuais, podendo ser arquivos em formato Open Virtualization Appliance (OVA), com a capacidade de criar um local próprio capaz de permitir a reprodução de ataques, além disso: • Os agentes devem ser compatíveis com sistemas operacionais Linux e Windows (Server e Professional); • Possibilitar a instalação de agentes ou máquinas OVA/ISO em ambientes de nuvem (cloud); • Permitir que os agentes possam ser removidos (desinstalados) de uma máquina ou ambiente e instalados em outro local reaproveitando uma mesma licença.	
2.6.2.1-11	Ser capaz de criar contas de usuários de forma local ou a autenticação e autorização de usuários por meio dos protocolos TACACS ou LDAP ou AD (Active Directory) ou mecanismos de autenticação e autorização utilizando credenciais corporativas no modelo de federação, usando o protocolo SAML.	
2.6.2.1-12	Ser capaz de simular ataques e validar as capacidades de prevenção e detecção para invasões em rede, gateways de web e e-mail, web application firewall (WAF), endpoints (EPP/EDR, antivírus) e Microsoft Active Directory, simular ataques em toda a cadeia de destruição cibernética (Cyber Kill Chain), incluindo infiltração, movimento lateral e exfiltração de dados, phishing, ransomwares, violações de segurança e ataques persistentes avançados (APTs).	
2.6.2.1-13	O portfólio de ameaças e ataques da solução deve ser baseado em frameworks de segurança cibernética, tais como MITRE ATT&CK, OWASP, CVSS ou NIST, e abranger todo o ciclo de ataque.	
2.6.2.1-14	Possuir portfólio de ameaças e ataques, templates ou cenários, que deverá ser atualizado continuamente contemplando ameaças atuais e emergentes, de forma manual e automática, com a opção de agendar a atualização em determinado período.	
2.6.2.1-15	Possibilitar a configuração de cenários de ataque, permitindo a seleção de quais ataques executar no teste.	



2.6.2.1-16	Permitir a criação de novas simulações de ataques e a customização destas a partir dos existentes em sua base de ameaças, de forma a permitir adaptações no comportamento e na ação dos ataques.	
2.6.2.1-17	Permitir o agendamento de simulações com a opção de execução contínua e automatizada.	
2.6.2.1-18	Possuir a instrumentação de indicadores de comprometimento (IOCs) provenientes de provedores de Threat Intelligence e/ou laboratório de inteligência de ameaça do fabricante da solução.	
2.6.2.1-19	Disponibilizar APIs (interfaces de programação de aplicações) que permitam sua integração com demais soluções de segurança do TRIBUNAL.	
2.6.2.1-20	Possuir integração com solução de monitoramento, detecção e resposta.	
2.6.2.1-21	Possuir dashboard com visualização dos resultados das simulações que retratem o nível de risco para cada fase da “Cyber Kill Chain”, baseado no MITRE ATT&CK com a possibilidade de customizar as visões apresentadas.	
2.6.2.1-22	Apresentar dados históricos de diferentes ataques simulados, bem como a visão de rastreamento.	
2.6.2.1-23	Possuir visualização por no mínimo: • Tipo de ataque simulado; • O que o artefato executou; • Data em que a simulação do ataque aconteceu; • Taxa de penetração.	
2.6.2.1-24	Permitir a realização de backup ou a opção de recuperação da solução, em caso de desastre, para no mínimo as configurações da solução de BAS.	
2.6.2.1-25	Podendo ser funcionalidade não disponível para o cliente, realizado sob demanda junto ao fabricante.	
2.6.2.1-26	Possuir registros que identifiquem o histórico completo de acessos (logins) e ações, por cada usuário ou grupo de usuários, incluindo as contas administrativas e com privilégios, podendo ser apresentado por meio de relatórios ou através de APIs ou scripts.	
2.6.2.1-27	Ter a opção de gerar relatórios após cada avaliação comparando com o resultado de testes anteriores, mostrando as vulnerabilidades mais críticas.	
2.6.2.1-28	Permitir exportar relatórios para formatos PDF e CSV.	
2.6.2.1-29	Apresentar relatório detalhando a ação do ataque simulado.	
2.6.2.1-30	Possuir capacidade de entregar relatório ou disponibilizar por meio de interface gráfica informações da sequência de execução do artefato malicioso, baseado na matriz do MITRE ATT&CK, bem como detalhar as alterações na máquina local e conexões externas executadas durante a simulação.	
2.6.2.1-31	Permitir exportar os logs da solução BAS, via API ou conectores, para a solução de SIEM.	
2.6.2.1-32	Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado.	



2.6.2.1-33	Possibilitar a execução ilimitada de todos os vetores de simulação disponíveis pela plataforma durante a vigência do mesmo.	
2.6.2.1-34	Possuir base ampla de recomendação de remediação possibilitando visualizar ações de correção, redução do impacto da vulnerabilidade/ataque e prevenção alinhados com as recomendações específicas dos fabricantes de elementos de segurança.	
2.6.2.1-35	A solução deve possuir atualização diária da base de malwares.	
2.6.2.1-36	Possuir simulações de campanhas de ameaças, com link para o relatório da identificação e descrição da ameaça em campo, descrevendo seus impactos e identificando as regiões do mundo afetadas pela campanha.	
2.6.2.1-37	Ser capaz de criar incidentes de forma manual e automática por meio de integrações com o SIEM.	
2.6.2.1-38	Possuir as seguintes opções para o formato do registro da hora dos eventos gerados com a integração do EDR: ISO 8601, UTC segundos, UTC milisegundos e UTC nanosegundos.	
2.6.2.1-39	Permitir customização de simulação de campanhas de ameaças, utilizando no mínimo os seguintes IOCs: hash de arquivos, nome do host, URLs e endereços IPv4.	
2.6.2.1-40	Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado, adotando como referência de mercado estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC, ISG Group.	
Item 2.7	GESTÃO DE IDENTIDADE	
2.7.1-1	Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado, adotando como referência de mercado estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC, ISG Group.	
2.7.1-2	A solução não deverá possuir EOL (End-of-life) e EOS (End-of-support) anunciados para um prazo superior a 36 meses.	
2.7.1-3	A solução poderá ser ofertada em ambiente de nuvem, em appliance virtual (virtualizado sob a plataforma VMware) ou appliance físico composto de hardware e software devidamente licenciado pela CONTRATADA.	
2.7.1-4	A solução deve possuir ferramenta de monitoração própria para que seja possível especificar limiares (thresholds) referente ao uso de memória, CPU, disco e banco de dados, e demais interações por meio do protocolo proprietário ou aberto (SNMP).	
2.7.1-5	Independente do modelo adotado, será necessário proporcionar uma retenção dos logs de até 180 dias, com gravações na ordem de 8 horas/dia, 5 dias por semana, no mínimo.	
2.7.1-6	A solução deve apoiar, no mínimo, os requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: • Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; • Proteger o acesso a dados pessoais sensíveis; • Responsabilizar pessoal e responder a incidentes;	



	• Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados.	
2.7.1-7	Apoiando os requisitos da LGPD, a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente.	
2.7.1-8	A solução deverá monitorar sessões, gravar, detectar, correlacionar e mitigar todos os comportamentos anormais de, pelo menos, 80 (oitenta) usuários administrativos simultâneos, acessando todos os sistemas-alvo do ambiente tecnológico, dentre eles Servidores Linux/Unix e Windows, banco de dados, appliances e demais ativos de rede e sistemas computacionais diversos.	
2.7.1-9	A solução deve atender no mínimo os sistemas-alvo os baseados nas seguintes tecnologias: • Sistemas Operacionais Linux/Unix e Microsoft Windows; • Microsoft Hyper-V e VMWare; • Contas de usuários de sistemas e de serviço; • Credenciais do Microsoft COM+, IIS; • Apache TomCat, RedHat Jboss, Wildfly, Nginx; • Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; • Contas de usuários e administradores de bancos de dados Microsoft SQL Server, PostgreSQL, MySQL; • Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) - switches, roteadores, balanceadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); • Contas de usuários e administradores de consoles de gerenciamento de servidores; • Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; • Credenciais de nuvem em VMWare ESXi, Azure, AWS, GCP, Microsoft 365.	
2.7.1-10	A solução deverá realizar a gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas.	
2.7.1-11	A solução deverá conceder acesso aos sistemas utilizando “Remote Desktop” e “SSH”, disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro	



	de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino.	
2.7.1-12	A solução deve permitir integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: • Integração e gestão de acessos privilegiados em contas de serviços em nuvem; • Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem.	
2.7.1-13	A solução deve possuir as sessões administrativas acessadas e monitoradas em tempo real, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada e possibilitando pesquisar ações específicas na sessão gravada.	
2.7.1-14	A solução deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios.	
2.7.1-15	A solução deve ser capaz de descobrir e alterar credenciais Microsoft Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, exibindo em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento.	
2.7.1-16	A solução deve gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado.	
2.7.1-17	A solução deve possuir funcionalidades de “AD Bridge” para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD.	



2.7.1-18	A solução deve provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente.	
2.7.1-19	A solução deve permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: • Permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; • Permitir a aprovação perante um agendamento de ações administrativas.	
2.7.1-20	Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução.	
2.7.1-21	Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas.	
2.7.1-22	A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP.	
2.7.1-23	A solução deve oferecer em sua console de gerenciamento diferentes visões e opções de acordo com as permissões dos usuários.	
2.7.1-24	A solução deve suportar métodos para registrar e relatar qualquer ação realizada, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail e integração com SIEM.	
2.7.1-25	Permitir o envio automático de logs para servidores syslog, de forma aderente ao disposto em RFC 5424 - The Syslog Protocol (IETF).	
2.7.1-26	A solução deve registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkouts, mudanças de delegação, relatórios e outras atividades, incluindo: • Registros de acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas; • Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários; • Alterações nas funções de delegação; • Adições, deleções e alterações de senhas gerenciadas pela solução; • Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; • Relatórios filtrados por período, tipo de operação, sistema, gerente e outros critérios.	
2.7.1-27	A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como: • Lista de sistemas gerenciados; • Senhas armazenadas/Contas gerenciadas; • Eventos de alteração de senha; • Permissões de acesso web;	



	• Auditoria de contas, sistemas e usuários.	
2.7.1-28	A solução deve realizar análise comportamental e mitigação de risco no ambiente crítico para Identidades Privilegiadas.	
2.7.1-29	A solução deverá realizar a identificação e o correlacionamento de ações, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução.	
2.7.1-30	A solução deve identificar e combinar ações que caracterizam abusos, montando perfis de comportamento anormal e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas, tais como, nova autenticação, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo: • Acesso privilegiado à solução durante horários irregulares. Detectado quando um usuário recuperar uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental; • Acesso privilegiado à solução durante dias irregulares. Detectado quando um usuário recuperar uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental; • Acesso excessivo a contas privilegiadas. Detectado quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental; • Acesso privilegiado à solução através de IP irregular ou desconhecido. Detectado quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental; • Acesso privilegiado não gerenciado. Detectado quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução; • Máquina acessada a partir de endereços IP incomuns; • Máquina acessada durante horários irregulares. Detectado quando uma máquina é acessada em um horário irregular, de acordo com seu padrão de utilização; • Acessos excessivos a uma máquina; • Acesso anômalo a várias máquinas. Detectado quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto; • Máquina incomum originando acesso; • Usuário incomum logando de uma máquina de origem conhecida; • Suspeita de roubo de credenciais. Detectado quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução; • Alteração de senha suspeita. Detectado quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução; • Atividades suspeitas detectadas durante uma sessão privilegiada. Detectado quando é identificada uma sessão privilegiada com atividades (comandos e anomalias na solução) definidas como suspeitas.	



	Para atendimento do item acima, poderão ser utilizados recursos integrados às soluções do Item 2.4 MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTAS A INCIDENTES DE SEGURANÇA.	
2.7.1-31	A solução deverá permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador.	
2.7.1-32	Ser capaz de, durante o processo de definição da política de composição de senha: • Gerar senhas aleatórias com extensão de 127 (cento e vinte e sete) caracteres ou mais; • Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos; • Especificar qual o tipo de caractere na composição das senhas a serem geradas; • Implementar controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada; • Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de acesso a esses grupos, onde esses privilégios de acesso possam ser atribuídos por critérios como tipo de dispositivo, sistemas operacionais, banco de dados e aplicativos de virtualização; • Garantir que a senha gerada seja diferente do nome da conta correspondente. Exemplo: se a credencial ou conta tem o nome “Administrador” a senha gerada jamais pode ser composta da mesma forma; • Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha.	
2.7.1-33	Realizar automaticamente a descoberta, detecção, importação e armazenamento no repositório seguro de chaves SSH em sistemas Linux, implementando: • Suporte a chaves criptográficas nos tamanhos 1024, 2048, 4096; • Auditoria e controle dos acessos às chaves por sistema de aprovações; • Reconciliação de chaves, renovando-as e armazenando-as novamente; • Conexão transparente a ativos da rede utilizando as chaves armazenadas; • Gerenciamento em grupos, permitindo que múltiplas máquinas herdem a mesma chave SSH.	
2.7.1- 34	Possibilitar colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador.	
2.7.1-35	Permitir o encerramento automatizado da sessão em caso de detecção de atividade suspeita de alta criticidade.	
2.7.1-36	Fornecer meio de integração para que soluções de terceiros também possam encerrar sessões suspeitas (ex: SIEM executa terminação de sessão).	



2.7.1-37	Criar relatórios que podem ser exportados em pelo menos um dos formatos editáveis: HTML, CSV, XLSX ou XLS.	
2.7.1-38	A solução deverá disponibilizar: • Mecanismo de retirada e devolução de contas e senhas compartilhadas; • Definição de tempo de validade, permitindo o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas; • Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido; • Troca de senhas por demanda, permitindo a troca de senhas nos sistemas gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (grupo de todos os sistemas operacionais UNIX, por exemplo).	
2.7.1-39	Suportar, através da interface Web para acesso e recuperação das senhas, de forma nativa, a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução.	
2.7.1-40	A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários, contas, configuração da solução e informações sobre os processos da solução.	
2.7.1-41	Permitir que os comandos executados em sistemas Linux monitorados sejam gravados em modo texto.	
2.7.1-42	Permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.	
2.7.1-43	Suportar em sua interface web e de administração métodos autenticação de duplo fator, compatíveis com os métodos a seguir: • Algoritmo de One-time Password, com pelo menos um dos aplicativos: Google Authenticator, Oauth, Authy, YubioAth, RSA SecureID, SAASPASS e 1Password; • Smart cards; • Tokens em geral; • Certificados Digitais.	
2.7.1-44	Possuir interface única, na mesma solução, para o gerenciamento de senhas e sessões.	
2.7.1-45	A solução deverá prover mecanismos de atualização de segurança sob demanda e com rastreabilidade dos pacotes instalados por meio de interface gráfica intuitiva (desejável).	
2.7.1-46	A solução não deve depender da instalação de agentes para realizar a troca de senhas e gravação de sessão.	
2.7.1-47	A solução deve ter uma console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas.	
2.7.2-1	A solução deverá possuir mecanismo de segurança que mantenha a entrega de credenciais em caso de queda da rede ou parada total do cofre digital, evitando assim a parada de aplicações críticas.	



2.7.2-2	Utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança e mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução.	
2.7.2-3	Todos os elementos que compõem a solução, devem ser instalados em regime de alta disponibilidade.	
2.7.2-4	Caso a solução seja na mobilidade on-premisse, a solução deve replicar as configurações em 02 (duas) localidades, de modo que, no evento de falha total de seus elementos instalados em uma localidade, a solução continue disponível via uso dos elementos da outra localidade, com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação.	
2.7.2-5	Todos os sistemas e recursos necessários para operação do módulo de cofre de senhas, deverão ser passíveis de plena utilização a partir de uma única localidade (site), em caso de contingência.	
2.7.2-6	Em caso de utilização de ambiente on-premisse, tanto os appliances virtuais quanto sistemas operacionais da solução devem ser “hardenizados” e protegidos com firewall interno.	
2.7.2-7	Deve permitir o backup e restore de seu banco de dados, bem como das configurações de software estabelecidas.	
2.7.2-8	Deve permitir a execução de tarefas de backup e criptografia sem a necessidade de agentes de terceiros ou parada do ambiente ou comprometimento de qualquer funcionalidade, provendo assim o maior nível possível de segurança e integridade dos dados a serem copiados.	
2.7.2-9	Deve permitir a execução de Backups automatizados, permitindo a programação/agendamento de horários e configuração de locais para seu armazenamento local e remoto.	
2.7.2-10	Deve ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), por meio de backup ou método análogo, para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas e dados gerenciados pela solução.	
2.7.2-11	Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos.	
2.7.2-12	Ainda que as gravações estejam armazenadas em locais diferentes, a solução deve permitir que essas evidências sejam consultadas a partir de qualquer console web instalada, de maneira centralizada.	
2.7.2-13	A solução deve ser disponibilizada com um SDK (Software Development Kit) que pode ser configurado para permitir que aplicações possam: • Atualizar informações de contas automaticamente no banco de dados de senhas; • Alterar senhas em texto-claro incorporados em aplicações de uma forma segura no banco de dados de senhas; • Solicitar as credenciais sob demanda via REST ou SOAP ao invés de utilizar credenciais estáticas; • Deverá integrar-se nativamente ao cofre digital da solução, utilizando sua mesma interface web.	



2.7.2-14	Deve possuir REST APIs detalhadamente documentadas no website do fabricante, estas APIs devem fornecer minimamente as funcionalidades de gestão das identidades, grupos e perfis, gestão de métodos de MFA, gestão de aplicações web, gestão de senhas, gestão do portal dos usuários finais e autenticação de usuários finais utilizando os métodos de MFA oferecidos.	
2.7.2-15	A solução deverá fornecer credenciais tanto por meio de acesso interativo via interface da solução na rede quanto por integração programática via APIs (Webservice).	
2.7.2-16	O uso de agente deve permitir instalação em múltiplos servidores web dos sistemas gerenciados pela solução, sem necessidade de aquisição de licenças, visando fornecer a melhor adaptação à arquitetura do CONTRATANTE.	
2.7.2-17	Deverá manter um cache atualizado das credenciais utilizadas localmente no servidor da aplicação, a fim de prevenir falhas na comunicação com o cofre digital e trazer velocidade às consultas.	
2.7.2-18	Deverá suportar a utilização de executável para scripts e aplicações nativas em plataforma Windows.	
2.7.2-19	Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em comandos Linux, comandos, janelas e aplicações Windows, Expressões regulares para comandos em geral e Eventos configurados manualmente, permitindo a atribuição de nível de risco customizado.	
2.7.2-20	Caso a solução fornecida faça uso das funcionalidades disponibilizadas pelas CALs (Client Access License) do serviço Microsoft Remote Desktop Services (RDS) para acessos através da mesma, a CONTRATANTE irá disponibilizar tal Infraestrutura, para que não seja afetada a experiência dos usuários.	
2.7.2-21	Permitir a opção de implementar o gerenciamento de troca de senhas em redes segregadas e remotas a fim de acomodar links de alta latência, redes isoladas (DMZ) e outras restrições semelhantes.	
2.7.2-22	A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH e HTTP/HTTPS.	
2.7.2-23	Integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas.	
2.7.2-24	Permitir o agrupamento lógico de credenciais, obedecendo uma hierarquia, a fim de simplificar a configuração e aplicação de políticas apropriadas para diferentes tipos de sistemas alvo, além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas.	
2.7.2-25	Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e realizar verificações agendadas e automáticas, a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino correspondam às mesmas senhas armazenadas no banco de dados da solução. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas notificando este evento.	



2.7.2-26	A solução deve conter meios de acessar os vídeos de gravações, incluindo: • Filtrar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado; • A função de gravação de sessões, devendo realizar o isolamento de sessões de acesso, atuando como um proxy/servidor de salto entre a máquina do usuário e o ativo a ser acessado.	
2.7.2-27	Permitir que os usuários solicitem acesso aos gestores através de interface web intuitiva.	
2.7.2-28	Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma.	
2.7.2-29	Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dasboards, filtros e gráficos configuráveis, sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.	
2.7.2-30	Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores.	
2.7.2-31	Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo: • E-mail com conteúdo do alerta; • Envio de alerta para solução SIEM.	
2.7.2-32	Possuir dashboards pré-configurados com informações e gráficos com as seguintes características: • Comportamento dos usuários na utilização das aplicações; • Visão sobre a segurança das aplicações; • Mapa com a geolocalização das autenticações; • Visão sobre o comportamento dos endpoints (Mobile e Computadores); • Visão sobre o comportamento das Identidades.	
2.7.2-33	A solução deve permitir a configuração de dashboards personalizados.	
2.7.3-1	A solução deve prover proteção e gerenciamento de secrets que atenda as demandas de segurança de credenciais e suas subcategorias, onde entende-se como secrets uma estrutura de dados que possa conter senhas, chaves privadas, tokens e chaves de APIs e ser entregue de maneira segura e criptografada para aplicações, contêineres e serviços.	
2.7.3-2	Deve criptografar todas as chaves privadas SSL utilizadas por quaisquer serviços da solução, ou utilizadas na criptografia da base de dados evitando que sejam armazenadas em texto claro no sistema de arquivos. A criptografia deve ocorrer antes da escrita em armazenamento persistente, evitando que informações sejam comprometidas em caso de acesso aos dados. Deve permitir que a chave master de criptografia seja armazenada e provida por soluções de HSM.	
2.7.3-3	A solução deverá atuar como gerador e intermediário (broker) de secrets para diversos clientes, como aplicações, contêineres e clientes de criptografia e possibilitar o armazenamento de múltiplas versões de um	



	mesmo secret. O fornecimento de secrets deve oferecer meios de controle de solicitante com múltiplos fatores, incluindo minimamente Tempo de vida (TTL) e restrições de IP/range.	
2.7.3-4	Os secrets devem ser modificáveis, com base em critérios de tempo de uso (Lease time) ou expiração, sendo que após expiração, a rotação ocorre de acordo com políticas definidas no sistema. Todo secret deve conter por padrão, pelo menos duas listas de acesso com papéis/grupos que podem ler o secret e que podem alterar o secret.	
2.7.3-5	Todos os registros de eventos de segurança como autenticação de clientes, solicitação de secrets, revogação de secrets, acesso de usuários, aplicações ou clientes a secrets, mudanças de permissão, deverão ser armazenados de maneira que impossibilite a sua alteração e se mantenha a correta integridade das evidências.	
2.7.3-6	As operações com secrets devem gerar trilha de auditoria contendo, no mínimo a identificação do cliente (usuário ou usuário sistêmico), a identificação do secret, horário (Timestamp completo), ação (leitura ou alteração) e se a ação foi permitida ou não.	
2.7.3-7	Deve utilizar definição de papéis (RBAC) para autorização de identidades de usuários e de aplicações onde possam ser definidos e relacionados entre si quando possível para usuários, grupos de usuários, usuários sistêmicos (máquinas, serviços e processos) e grupos de usuários sistêmicos.	
2.7.3-8	Todas as operações envolvendo usuários e grupos sistêmicos e não-sistêmicos, políticas e secrets, incluindo a criação, leitura e alteração, devem ser feitas via linguagem aberta de serialização YAML.	
2.7.3-9	A obtenção de secrets deve ser permitida por diversos meios, incluindo, pelo menos, linha de comando (CLI) e RestAPI. Os secrets deverão ser disponibilizados unicamente para as aplicações ou serviços que os consomem, sendo que em hipótese alguma, devem ser disponibilizados no nível do sistema operacional ou “namespaces” acessíveis por outras aplicações.	
2.7.3-10	A solução deverá guardar e rotacionar os secrets no repositório central de credenciais da solução, sem necessidade de criação de novo ambiente de administração de credenciais, mantendo os mesmos requisitos de segurança já definidos para aquela solução.	
2.7.3-11	Deve oferecer recursos de redundância, alta disponibilidade e suporte a balanceamento de carga se utilizando da infra-estrutura disponibilizada pela CONTRATANTE. A alta disponibilidade deve conter funcionalidade de replicação automática entre as bases da solução, oferecendo pelo menos 2 réplicas. O conjunto de réplicas deve oferecer funcionalidade de Failover automático, onde uma das réplicas assumirá a operação em caso de problemas. Deve haver funcionalidade de backup seguro do conteúdo armazenado e configurações do produto, possibilitando a prática de Disaster Recovery.	
2.7.3-12	Para que não haja sobrecarga nem exposição do repositório central da solução e suas redundâncias, a solução deve oferecer componentes que absorvam a carga de requisições. Esses componentes devem agregar capacidade de requisições por segundo de maneira quantitativa ao total da solução.	



TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ