TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA **Núcleo de Licitação**	
Processo Administrativo nº TJ-ADM-2022/19737	**PREGÃO ELETRÔNICO Nº 068/2022**
Objeto	Contratação de solução de segurança da informação, composta de software de segurança para usuário final e cargas de trabalho híbridas, proteção contra ameaças avançadas incluindo fornecimento de *appliance*, proteção contra ameaças de nuvem e gerenciamento de conformidade, com detecção e resposta e gerenciamento proativo e corretivo das soluções, para o Tribunal de Justiça do Estado da Bahia, conforme exigências estabelecidas neste documento e seus anexos.
A participação neste pregão eletrônico ocorrerá exclusivamente por meio do sistema eletrônico do Banco do Brasil, com a digitação da senha privativa da licitante e subsequente encaminhamento da proposta inicial de preços, a partir da data da liberação do Edital até o horário da abertura da sessão pública.	
Endereços eletrônicos: www.licitacoes-e.com.br. Portal eletrônico do Tribunal de Justiça do Estado da Bahia, www.tjba.jus.br , opção licitação/pesquisa.	
Disponibilidade do Edital: O edital está disponível através do link www.licitacoes-e.com.br e do portal eletrônico do Tribunal de Justiça do Estado da Bahia, www.tjba.jus.br , opção licitação/pesquisa.	
Dúvidas e Esclarecimentos: 1. Os interessados poderão encaminhar questionamentos e impugnações ao Núcleo de Licitação, através do endereço eletrônico ncl@tjba.jus.br ou através de fac-símile (71 – 3372-1602/1617/1877). As consultas respondidas pelo pregoeiro estarão disponíveis na página www.licitacoes-e.com.br, no campo “MENSAGENS”, no link correspondente a este edital, para ciência de qualquer interessado 2. Os licitantes deverão acompanhar o andamento das licitações através do endereço www.tjba.jus.br e na página www.licitacoes-e.com.br em todas as suas etapas, até a sua finalização (homologação), ficando responsáveis pelo ônus decorrente da inobservância de quaisquer mensagens/informações emitidas pelo Núcleo de Licitação ou pregoeiro.	
Endereço	**Núcleo de Licitação** 5ª Av. do Centro Administrativo da Bahia, Prédio do Tribunal de Justiça da Bahia, 1° Andar, Sala 119, CEP:41.745-970, Telefones: 71-3372-1600/1601/1699/1636.

TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA

Núcleo de Licitação

EDITAL – PREGÃO ELETRÔNICO Nº068/2022

1. PREÂMBULO

O **TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA**, órgão do Poder Judiciário, inscrito no CNPJ/MF sob nº 13.100.722/0001-60, situado na 5ª Av. do CAB (Centro Administrativo da Bahia - CAB), nº 560, Salvador-Bahia, CEP 41.746-000, através do Núcleo de Licitação, situado no Edifício-Sede, 1º andar, Norte, sala 119, torna público a quantos o presente edital virem ou dele conhecimento tomarem, que realizará licitação **PE 068/2022,** autorizada no **processo TJ-ADM-2022/19737,** na modalidade **PREGÃO, na forma eletrônica**, do tipo **menor preço GLOBAL**, conduzida por Pregoeiro designado através do Decreto nº 532/2022, publicado no Diário da Justiça Eletrônico, edição de 27/07/2022. Esta licitação obedecerá, integralmente, as disposições da Lei Estadual nº 9.433/05 e suas alterações, Lei nº 12.846/2013, Lei 13.709/2018, Lei Complementar nº 123/2006, das Leis Federais nºs 10.520/02 e 8.666/93, no que for pertinente, **do Decreto Estadual nº 19.896/2020**, Resolução nº 07/2005, alterada pela Resolução nº 229/16 do Conselho Nacional de Justiça, além dos Decretos Judiciários nºs 12/03, 44/03, 13/06, 28/08, 784/14 e 813/19 do Tribunal de Justiça do Estado da Bahia.

1.1. Local, data e horários:

Acolhimento das propostas a partir de:	**18/03/2023 às 08:00 horas.**
Abertura das propostas:	**31/03/2023 às 09:30 horas.**
Início da sessão de disputa de lances:	**31/03/2023 às 10:00 horas.**
Modo de Disputa (Art. 11, §5º do Decreto Estadual nº 18.896/2020)	Aberto
Intervalo mínimo de diferença entre lances (Art. 11, §3º do Decreto Estadual nº 19.896/2020)	Sim. Intervalo mínimo de R$1.000,00 entre lances.
Intervalo mínimo de diferença entre lances (Art. 11, §4º do Decreto Estadual nº 19.896/2020)	Sim. Intervalo mínimo de 5 segundos entre lances.
Tempo de disputa	Etapa de lances aberta: Até 10 min Prorrogação automática se houver lance nos últimos 02 (dois) minutos (determinado pelo sistema).
Endereço eletrônico	www.licitacoes-e.com.br

Obs.: Será sempre considerado o horário de Brasília (DF) para todas as indicações de tempo constantes neste edital.

1.2. São partes indissociáveis deste Edital os seguintes anexos:

Anexo I - Termo de Referência
Anexo II – Modelo de Proposta Comercial
Anexo III – Modelo de Termo de Confidencialidade
Anexo IV -. Modelo de Termo de Designação de Preposto
Anexo V - Modelo de Declaração de Elaboração Independente da proposta
Anexo VI - Modelo de Declaração de Responsabilidade
Anexo VII - Modelo de Declaração de Enquadramento e de Atendimento às Exigências de Habilitação;
Anexo VIII - Modelo de Declaração de Cumprimento ao art. 1º do Decreto Judiciário nº 95/2014 e Resolução do CNJ nº 229/16
Anexo IX – Modelo de Procuração para a prática de atos Concernentes ao Certame.
Anexo X - Modelo de Declaração de Pleno Conhecimento e de Veracidade dos Documentos.
Anexo XI – Modelo de Declaração de Desimpedimento de Licitar e/ou Contratar;
Anexo XII – Modelo de Minuta do Contrato/ Termo De Cumprimento Da Lei Geral De Proteção De Dados;
Anexo XIII - Modelo de Declaração da Proteção ao Trabalho do Menor;
Anexo XIV - Modelo de Declaração de não inscrição no cadastro de empregadores flagrados explorando trabalhadores.
Anexo XV - Modelo de Declaração Não condenação por infringir as leis de combate à discriminação de raça ou de gênero.

2. OBJETO DA LICITAÇÃO

2.1. A presente licitação tem por objeto a contratação de solução de segurança da informação, composta de software de segurança para usuário final e cargas de trabalho híbridas, proteção contra ameaças avançadas incluindo fornecimento de *appliance*, proteção contra ameaças de nuvem e gerenciamento de conformidade, com detecção e resposta e gerenciamento proativo e corretivo das soluções, para o Tribunal de Justiça do Estado da Bahia, conforme exigências estabelecidas neste documento e seus anexos.

2.2. Em caso de discordância existente entre as especificações deste objeto descritas no SISTEMA DO BANCO DO BRASIL e as especificações constantes deste Edital, prevalecerão as últimas.

2.3. Com base nas cotações recolhidas, o valor máximo aceitável para esta contratação, conforme definido no item 2.10.01. do Anexo I – Termo de Referência, é de R$14.151.349,34 (quatorze milhões, cento e cinquenta e um mil, trezentos e quarenta e nove reais e trinta e quatro centavos), pelo período de 24 (vinte e quatro) meses.

2.3.1. A despesa decorrente do presente instrumento será atendida através da Unidade Orçamentária 02.04.601, Unidade Gestora 0004-SETIM, Atividade 2002/2034/2035/5051/5052/5054, Elemento de Despesa 3.3.90.40/4.4.90.52, Subelemento 40.02/40.06, Fonte 113/120/313/320/326.

3. CONDIÇÕES GERAIS DE PARTICIPAÇÃO NA LICITAÇÃO

3.1. Somente serão admitidos a participar desta Licitação os interessados previamente credenciados perante o Banco do Brasil, que atenderem a todas as exigências de habilitação contidas neste edital e seus anexos.

3.2. Não poderão participar deste Pregão, na forma eletrônica:

3.2.1. Empresas que estejam suspensas temporariamente de participar e de licitar com a Administração Pública ou ainda as declaradas inidôneas, na forma dos incisos II e III do art. 186 da Lei Estadual nº 9.433/05;

3.2.2. Em consonância com o art. 200 da Lei estadual nº 9.433/05, fica impedida de participar de licitações e de contratar com a Administração Pública a pessoa jurídica constituída por membros de sociedade que, em data anterior à sua criação, haja sofrido penalidade de suspensão do direito de licitar e contratar com a Administração ou tenha sido declarada inidônea para licitar e contratar e que tenha objeto similar ao da empresa punida.

3.2.3. Consoante o art. 18 da Lei estadual nº 9.433/05, não poderá participar, direta ou indiretamente, da licitação, da execução de obras ou serviços e do fornecimento de bens a eles necessários os demais agentes públicos, assim definidos no art. 207 do mesmo diploma, impedidos de contratar com a Administração Pública por vedação constitucional ou legal.

3.2.4. É defeso ao servidor público transacionar com o Estado quando participar de gerência ou administração de empresa privada, de sociedade civil ou exercer comércio, na forma do inc. XI do art. 176 da Lei estadual nº 6.677/94.

3.2.5. É vedado ao agente político e ao servidor público de qualquer categoria, natureza ou condição, celebrar contratos com a Administração direta ou indireta, por si ou como representante de terceiro, sob pena de nulidade, ressalvadas as exceções legais, conforme o art. 125 da Lei Estadual nº 9.433/05.

3.2.6. Não poderão participar desta licitação, pessoas jurídicas que não explorem atividade compatível com o objeto desta licitação.

3.3. Participação de consórcios e subcontratação:

3.3.1. O Tribunal de Justiça do Estado da Bahia não aceitará a subcontratação de outras empresas nem a formação de consórcio para a prestação dos serviços licitados, devendo uma única empresa assumir a responsabilidade integral pela execução.

3.4. Participação de Cooperativas:

3.4.1. Não será admitida a participação de Sociedades Cooperativas, conforme SÚMULA Nº 281 do TCU; Art. 10, §5º da Lei 12.690/2012; Termo de Conciliação Judicial firmado entre o Ministério Público do Trabalho e a União, de 5 de junho de 2003 e Instrução Normativa SGMPDG Nº 5 de 25 de maio de 2017 com as alterações da IN n.º 7 de 20 de setembro de 2018.

3.5. Participação de Organização da Sociedade Civil de Interesse Público (OSCIP) e Instituições sem fins lucrativos:

3.5.1. Não será admitida a participação de Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014, 1.557/2014 e 4.652/2015-TCU-Plenário), bem como instituições sem fins lucrativos (parágrafo único do art. 12 da Instrução Normativa/SEGES nº 05/2017).

4. IMPUGNAÇÃO DO ATO CONVOCATÓRIO E DOS PEDIDOS DE ESCLARECIMENTOS

4.1. DAS IMPUGNAÇÕES

4.1.1. Qualquer pessoa poderá impugnar os termos do edital do pregão até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública. **[NOTA: art. 13 do Decreto nº 19.896/20]**

4.1.1.1 A petição deverá ser dirigida a(o) pregoeiro(a) responsável pela condução do certame, podendo ser encaminhada na forma eletrônica, através do e-mail: **ncl@tjba.jus.br**, **até as 23:59h do último dia do prazo**, ou protocolada na Sede do TJBA situada à 5ª Avenida, 1º andar, sala nº 119 Norte, Centro Administrativo da Bahia Salvador – BA, CEP: 41.745-970, **até às 18 horas do último dia do prazo** (observado o horário de funcionamento do protocolo do TJBA).

4.1.2. A impugnação não possui efeito suspensivo e caberá ao pregoeiro decidir no prazo de 02 (dois) dias úteis, contado da data de recebimento da impugnação. [NOTA: art. 13, §1o, do Decreto no 19.896/20]

4.1.3. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro nos autos do processo de licitação. [NOTA: art. 13, §2o, do Decreto no 19.896/20]

4.1.4. O pregoeiro poderá solicitar a manifestação dos setores técnicos, a fim de subsidiar a decisão quanto às impugnações, promovendo a oitiva, quando necessário, do órgão legal de assessoramento jurídico. [NOTA: art. 13, §3o, do Decreto no 19.896/20]

4.1.5. Se reconhecida a procedência das impugnações, as modificações do edital serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes. [NOTA: art. 15 do Decreto no 19.896/20]

4.1.6. Decairá do direito de impugnar os termos deste edital perante a Administração a licitante que não o fizer até o terceiro dia útil que anteceder a data prevista para a abertura da Sessão Pública, apontando as falhas ou irregularidades que o viciou.

4.1.7. As respostas às impugnações serão disponibilizadas em meio eletrônico, através do site deste Tribunal de Justiça do Estado da Bahia, no endereço www.tjba.jus.br, opção licitacao/pesquisa, e do sistema Licitacoes-e do Banco do Brasil.

4.2. DOS PEDIDOS DE ESCLARECIMENTOS

4.2.1. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao pregoeiro até 03 (três) dias úteis anteriores da data fixada para a realização da sessão pública do pregão. **[NOTA: art. 14 do Decreto no 19.896/20]**

4.2.1.1. A solicitação deverá ser dirigida a(o) pregoeiro(a) responsável pela condução do certame, podendo ser encaminhada na forma eletrônica, através do e-mail: **ncl@tjba.jus.br**, **até as 23:59h do último dia do prazo**, ou protocolada na Sede do TJBA situada à 5ª Avenida, 1º andar, sala nº 119 Norte, Centro Administrativo da Bahia Salvador – BA, CEP: 41.745-970, **até às 18 horas do último dia do prazo** (observado o horário de funcionamento do protocolo do TJBA).

4.2.2. O pregoeiro responderá aos pedidos de esclarecimentos no prazo de 02 (dois) dias úteis, contado da data de recebimento do pedido, e suas respostas vincularão os participantes e a Administração Pública Estadual. **[NOTA: art. 14, §1o, do Decreto no 19.896/20]**

4.2.3. O pregoeiro poderá solicitar a manifestação dos setores técnicos, a fim de subsidiar a decisão quanto aos pedidos de esclarecimentos, promovendo a oitiva, quando necessário, do órgão legal de assessoramento jurídico. **[NOTA: art. 14, §2o, do Decreto no 19.896/20]**

4.2.4. Se na resposta aos pedidos de esclarecimentos verificar-se a necessidade de modificações do edital, estas serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes. **[NOTA: art. 15 do Decreto no 19.896/20]**

4.2.5. As respostas aos questionamentos serão disponibilizadas em meio eletrônico, através do site deste Tribunal de Justiça do Estado da Bahia, no endereço www.tjba.jus.br, opção licitacao/pesquisa, e do sistema Licitacoes-e do Banco do Brasil.

5. DO PROCEDIMENTO DA LICITAÇÃO

DO CREDENCIAMENTO

5.1. O Banco do Brasil atuará como órgão provedor do sistema eletrônico.

5.1.1. O site, dia e hora para recebimento das propostas e início da sessão pública estão indicados na Capa do Edital.

5.2. O credenciamento do licitante será realizado pelo Banco do Brasil, no prazo máximo de até 03 (três) dias úteis após a formalização do pedido e da entrega da documentação necessária.

5.3. O credenciamento dar-se-á pela atribuição de senha pessoal e intransferível para acesso ao Sistema de Pregão Eletrônico, obtidas junto às agências do Banco do Brasil S.A.

5.4. O credenciamento junto ao provedor do sistema funcionará como assinatura eletrônica e implicará para o licitante:

a) presunção de sua capacidade técnica para a realização das transações inerentes ao Pregão Eletrônico;

b) obrigar-se pelas transações efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiros seus lances e propostas, validando todos os atos praticados;

c) dever de acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, responsabilizando-se pelo ônus decorrente da perda de negócios por inobservância de qualquer mensagem emitida pelo sistema eletrônico ou de sua desconexão.

5.5. Reputa-se credenciada a pessoa natural regularmente designada para representar a licitante no processo licitatório.

5.6. Cada licitante poderá credenciar apenas um representante e cada representante somente poderá representar uma única licitante.

5.7. O credenciamento do usuário será pessoal e intransferível para acesso ao sistema, sendo a licitante responsável por todos os atos praticados.

5.8. O uso da senha de acesso pelo licitante é de sua exclusiva responsabilidade, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao Tribunal de Justiça-TJ/BA responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros. A perda da senha ou a quebra do sigilo deverá ser comunicado imediatamente ao provedor do sistema, para imediato bloqueio de acesso.

5.9. As licitantes interessadas na concessão de tratamento diferenciado assegurado pela Lei Complementar nº 123/06 deverão estar previamente cadastradas no sistema indicado no 5.1 acima, como microempresas ou empresas de pequeno porte.

5.10. Informações complementares sobre credenciamento no sistema poderão ser obtidas pelos telefones: 4004001 ou 0800-72900001 (Suporte Técnico).

DO LICITANTE

5.11. Caberá à licitante interessada em participar do pregão, na forma eletrônica: **[NOTA: art. 17 do Decreto no 19.896/20]**

a) credenciar-se previamente no sistema eletrônico utilizado no certame;
b) remeter, no prazo estabelecido, exclusivamente via sistema eletrônico, os documentos de habilitação e a proposta e, quando necessário, os documentos solicitados conforme estabelecido neste edital;
c) responsabilizar-se formalmente pelas transações efetuadas em seu nome, assumir 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 da senha, ainda que por terceiros;
d) acompanhar as operações no sistema eletrônico durante o processo licitatório e responsabilizar-se pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão;
e) comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a inviabilidade do uso da senha, para imediato bloqueio de acesso;
f) utilizar a chave de identificação e a senha de acesso para participar do pregão na forma eletrônica.

5.12. O credenciamento do usuário implica em sua responsabilidade legal e na presunção de capacidade técnica para realização das transações inerentes ao pregão.

6. APRESENTAÇÃO ELETRÔNICA DAS PROPOSTAS DE PREÇOS E DOCUMENTOS DE HABILITAÇÃO

6.1. Após a divulgação do edital no sítio eletrônico, **as licitantes encaminharão, exclusivamente por meio do sistema eletrônico, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço**, conforme as datas e horários estabelecidos no instrumento convocatório, observando-se o que se segue: **[NOTA: art. 18, caput, do Decreto no 19.896/20]**

6.1.1. A proposta de preços de cada licitante, a que se refere o **item 6.1**. acima, se restringe ao preenchimento do formulário eletrônico em sistema.

6.1.1.1. A licitante deverá preencher o formulário eletrônico apresentado na tela com os dados pertinentes à sua proposta de preços, cadastrando em sistema a(s) oferta(s) relativa(s) a todos os itens/lotes que irá disputar (item a item), **vedada a identificação da proponente ou do seu representante legal, sob pena de desclassificação**.

6.1.1.2. Para fins de classificação inicial de proposta (antes da disputa de lances), será considerado somente o conteúdo contido no formulário eletrônico de proposta, preenchido por cada licitante através de campos próprios do sistema. Por conseguinte, será considerado não apresentado documento de proposta de preços inicial, eventualmente inserido em sistema sob a forma de anexo, antes da abertura da sessão pública.

6.1.1.3. Para fins de aceitação de proposta de preços da(s) licitante(s) melhor(es) classificada(s), após a finalização da disputa de lances, serão considerados os documentos enviados sob a forma de anexo, após a convocação pelo(a) pregoeiro(a), nos termos do **item 9.10 deste edital**.

6.1.2. As licitantes também deverão remeter nesta oportunidade, **exclusivamente via sistema eletrônico**:

a) proposta escrita de preços, preferencialmente de acordo com o modelo do Anexo II – Modelo de Proposta Comercial;
b) declaração de elaboração independente de proposta e de inexistência de impedimento à participação no certame, preferencialmente de acordo com o modelo constante deste edital;
c) Declaração de Enquadramento (Lei nº 123/06), preferencialmente de acordo com o modelo constante deste edital**;**
d) declaração de pleno conhecimento e de veracidade dos documentos, preferencialmente de acordo com o modelo constante deste edital**;**
e) Declaração de Desimpedimento de Licitar ou contratar com a Administração direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, abrangendo inclusive as entidades com personalidade jurídica de direito privado sob controle do poder público e as fundações por ele instituídas ou mantidas (art. 185, III, da Lei Estadual 9.433/05), preferencialmente de acordo com o modelo constante deste edital;
f) Declaração de Cumprimento ao art. 1º do Decreto Judiciário nº 95/2014, prevista no Anexo VIII; e
g) procuração, se for o caso, por instrumento público ou particular, este último acompanhado da prova da legitimidade de quem outorgou os poderes.

6.1.3. Os documentos exigidos para habilitação, conforme item 7.7 do edital deverão ser enviados nesta fase, **exclusivamente via sistema eletrônico**, observando-se o que se segue:

6.1.3.1 As licitantes cadastradas no Cadastro Unificado de Fornecedores do Estado da Bahia poderão deixar de apresentar os documentos de habilitação que constem no referido Cadastro, observado o disposto neste edital, para a confirmação das suas condições habilitatórias. [NOTA: art. 18, §1o, do Decreto no 19.896/20]

6.1.3.2 Os documentos exigidos para habilitação que não estejam contemplados no Registro Cadastral, ou que dele constem como vencidos, deverão ser enviados nesta fase, cabendo ao licitante certificar-se da regularidade de sua documentação. [NOTA: art. 18, §2o, do Decreto no 19.896/20]

6.1.4 O envio da proposta, acompanhada dos documentos de habilitação exigidos no edital, nos termos do disposto no item 6.1 ocorrerá por meio de chave de acesso e senha. [NOTA: art. 18, §3o, do Decreto no 19.896/20]

6.1.5 A licitante declarará, em campo próprio do sistema eletrônico, o cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências do edital. [NOTA: art. 18, §4o, do Decreto no 19.896/20]

6.1.6 A falsidade da declaração de que trata o item 6.1.5 sujeitará o licitante às sanções previstas na legislação pertinente. [NOTA: art. 18, §5o, do Decreto no 19.896/20]

6.1.7 Os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema eletrônico, até a data e o horário estabelecidos no edital para a sua apresentação. [NOTA: art. 18, §6o, do Decreto no 19.896/20]

6.1.8 Na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, observado o disposto no item 6.1 não haverá ordem de classificação das propostas. [NOTA: art. 18, §7o, do Decreto no 19.896/20]

6.1.9 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances. [NOTA: art. 18, §8o, do Decreto no 19.896/20]

6.1.10. A vedação à inclusão de novo documento, prevista no art. 30, §3º do Decreto Estadual nº 19.896/2020, bem como no art. 43, §3º da Lei Federal nº 8.666/93, não alcança documento destinado a atestar condição de habilitação preexistente à abertura da sessão pública, apresentado em sede de diligência (Acórdãos nºs 1211, 2443 e 2568, todos expedidos em 2021 pelo Plenário do TCU)

7. DA PROPOSTA COMERCIAL E DOS DOCUMENTOS DE HABILITAÇÃO

7.1. Os documentos relativos à proposta e à habilitação serão apresentados em formato digital, sob exclusiva responsabilidade dos proponentes quanto à sua validade.

7.1.1. Em caso de dúvida quanto à autenticidade dos documentos, o pregoeiro poderá solicitar a apresentação dos documentos em original ou cópia autenticada, para verificação.

7.1.2. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.

7.1.3 A falsidade dos documentos apresentados sujeitará a licitante às sanções previstas na legislação pertinente.

7.2. As certidões extraídas pela internet somente terão validade se confirmada sua autenticidade.

7.3. Como condição específica para participação do pregão por meio eletrônico, é necessário, previamente, o credenciamento pelos licitantes no sistema indicado no PREÂMBULO, através da atribuição de chave de identificação e/ou senha individual.

7.4. A participação no pregão eletrônico dar-se-á por meio do acesso da licitante exclusivamente por meio do sistema disponibilizado.

7.5. Para a habilitação dos interessados na licitação, exigir-se-ão, exclusivamente, os documentos relacionados no instrumento convocatório.

7.5.1 As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar no 123/06, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição.

7.6. PROPOSTA COMERCIAL:

7.6.1 O proponente deverá elaborar a sua proposta escrita de preços de acordo com as exigências constantes do Termo de Referência, em consonância com o modelo proposto neste convocatório, expressando os valores em moeda nacional – reais e centavos, em 02 (duas) casas decimais, ficando esclarecido que não serão admitidas propostas alternativas. Caso o resultado final resulte em dízima, a licitante deverá apresentar uma nova proposta, no prazo estabelecido, que resulte em apenas duas casas decimais, cujo valor deverá ser inferior ao inicialmente proposto.

7.6.1.1. Ocorrendo divergência entre o preço por item em algarismo e o expresso por extenso, será levado em conta este último.

7.6.1.2. A formulação da proposta implica para a proponente a observância dos preceitos legais e regulamentares em vigor, tornando-a responsável pela fidelidade e legitimidade das informações e dos documentos apresentados.

7.6.1.3. O licitante deverá elaborar a sua proposta de preços com base no Termo de Referência e Anexos, sendo de sua exclusiva responsabilidade o levantamento dos serviços/bens, quantitativos, custos e tudo mais que for necessário para o cumprimento total das obrigações decorrentes da execução do objeto da licitação.

7.6.1.3.1. Será desclassificada, após a etapa de lances e negociação, a proposta que consignar valor global superior aos praticados no mercado, de acordo com o valor máximo aceitável para esta contratação, conforme definido no item 2.10.1 do Anexo I – Termo de Referência e item 2.3. deste Edital.

7.6.1.3.2. Não serão aceitas propostas cujo valor global seja superior aos limites máximos determinados no item 2.10.1 do Anexo I – Termo de Referência e item 2.3. deste Edital, devendo ser respeitados não apenas o máximo global, mas também os limites máximos por item.

7.6.2. Na Proposta de Preços escrita, o licitante deverá informar:

a) O prazo de validade da proposta comercial será de, no mínimo, 90 (noventa) dias a contar da data da sua apresentação, ainda que a licitante estipule prazo menor ou que não a consigne, facultado aos proponentes estender tal validade por prazo superior. Findo o prazo de validade, os licitantes ficarão liberados dos compromissos assumidos se não for efetivada a convocação dos mesmos para a assinatura do contrato.

b) No valor da proposta deverão estar contempladas todas e quaisquer despesas necessárias ao fiel cumprimento do objeto desta licitação, inclusive todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da Contratada, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, fretes, seguros, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela Contratada das obrigações, devendo o preço ofertado corresponder, rigorosamente às especificações do objeto licitado.

7.6.3. A responsabilidade quanto ao serviço ofertado é exclusivamente do licitante, que deverá certificar-se se o mesmo atende às exigências do instrumento convocatório sob pena de, em caso negativo, sofrer as sanções previstas no **item 18 deste Edital.**

7.6.4. Todas as características descritas pelas licitantes devem guardar compatibilidade com as especificações exigidas neste instrumento convocatório, devendo o produto, serviço ou componente ofertado ser claramente descrito de forma visual e/ou escrita.

7.6.5. Os preços cotados deverão ser referidos à data de recebimento das propostas, considerando a condição de pagamento à vista, não devendo, por isso, computar qualquer custo financeiro para o período de processamento das faturas.

7.6.6. Não será permitida previsão de sinal, ou qualquer outra forma de antecipação de pagamento na formulação das propostas, devendo ser desclassificada, de imediato, a proponente que assim o fizer.

7.6.7.A apresentação da proposta implica para a licitante a observância dos preceitos legais e regulamentares em vigor, bem como a integral e incondicional aceitação de todos os termos e condições deste Edital, sendo responsável pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer ase da licitação.

7.6.8. Não será considerada qualquer oferta de vantagem não prevista neste instrumento, nem propostas com preço global ou unitário simbólico, irrisório ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos.

7.6.9. O Tribunal de Justiça da Bahia não se enquadra como contribuinte do ICMS, conforme estabelecido no art. 4º da Lei Complementar nº 87/96 e no art. 36 do RICMS do Estado da Bahia, aprovado pelo Decreto nº 6.284/97.

7.6.10 Qualquer elemento que possa identificar a licitante importa desclassificação da proposta, sem prejuízo das sanções previstas nesse Edital.

7.6.11. A disputa será pelo PREÇO GLOBAL do lote, devendo os licitantes respeitarem os preços máximos aceitáveis para cada item, para o período de 24 (vinte e quatro) meses de vigência do contrato, conforme item 2.10.1. do Anexo I do Edital.

7.6.11.1. Não serão aceitas propostas cujos valores por item sejam maiores que os valores referenciais, por item, listados na tabela constante do item 2.10.1. do Anexo I -Termo de Referência e item 2.3. deste Edital**.**

DOS DOCUMENTOS DE HABILITAÇÃO

7.7. HABILITAÇÃO:

7.7.1. Para a habilitação dos interessados, exigir-se-ão os documentos relativos a:

7.7.1.1. HABILITAÇÃO JURÍDICA, comprovada mediante a apresentação:

a) inscrição no Registro Público no caso de empresário individual.

b) em se tratando de sociedades empresárias, do ato constitutivo, estatuto ou contrato social, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados, quando for o caso, dos documentos societários comprobatórios de eleição ou designação e investidura dos atuais administradores.

c) no caso de sociedades simples, do ato constitutivo, estatuto ou contrato social, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados dos atos comprobatórios de eleição e investidura dos atuais administradores.

d) decreto de autorização, no caso de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

7.7.1.2. A REGULARIDADE FISCAL E TRABALHISTA, comprovada mediante a apresentação de:

7.7.1.2.1. Regularidade Fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ;

b) Prova de inscrição no Cadastro de Contribuinte Municipal (para licitação de serviços) , relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio ou sede do licitante;

d) prova de regularidade para com a Fazenda Federal, inclusive INSS.

e) Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), mediante a apresentação do Certificado de Regularidade do FGTS – CRF.

1. A prova da inscrição a que se referem os itens **"a"** e **"b" da regularidade fiscal e trabalhista** será suprida com a apresentação das certidões a que se referem os itens **"c"** e **"d"**, respectivamente, se estas contiverem o número de inscrição do licitante.

7.7.1.2.2. Regularidade Trabalhista:

a) Certidão Negativa (ou positiva com efeitos de negativa) de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho, em cumprimento à Lei nº 12.440/2011 e Resolução Administrativa nº 1.470/2011.

2. As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar nº 123/06, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, cumprindo-lhes assinalar a sua condição nos campos correspondentes na **Declaração Quanto à Regularidade Fiscal e Trabalhista.**

7.7.1.3. QUALIFICAÇÃO TÉCNICA, comprovada mediante apresentação de:

7.7.1.3.1. Documento de comprovação de que a licitante é revendedora ou distribuidora autorizada do fabricante.

7.7.1.3.2. atestado (s) de capacidade técnica em nome da empresa, emitido (s) por pessoa (s) jurídica (s) de direito público ou privado, que, individualmente ou somados, comprove (m) o desempenho satisfatório na execução dos serviços abaixo listados:

a) Fornecimento de, no mínimo, 3.500 licenças de *software* de segurança TrendMicro para *Endpoint*, compatível com o item 1 da solução, constante na tabela 02 do Anexo I - Termo de Referência;
b) Fornecimento de, no mínimo, 250 licenças de solução de segurança para servidores, compatível com o item 2 da tabela 02 do Anexo I - Termo de Referência;
c) Fornecimento e Instalação de, no mínimo, 1 *Appliance* de segurança do Tipo Inspeção de rede com o mínimo de 1 Gbps de *Throughput*;
d) Prestação de serviço gerenciado de suporte especializado nas soluções TrendMicro por, no mínimo, 12 meses;

7.7.1.3.2.1. Todas as informações citadas acima deverão constar de forma explícita no (s) atestado (s).

7.7.1.3.2.2. Admite-se mais de um atestado com vistas a comprovar o atendimento a todos os requisitos de capacidade técnica que asseguram a similaridade do objeto.

7.7.1.3.2.3. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da licitante. Serão consideradas como pertencentes ao mesmo grupo empresarial, as empresas controladas ou controladoras da empresa licitante, e ainda as que tenham pelo menos uma pessoa física ou jurídica como sócia em comum.

7.7.1.3.2.4. Somente serão aceitos atestados referentes a contratos já encerrados ou referentes a contratos cuja execução já tenha alcançado pelo menos 50% do volume de seu respectivo objeto, no que concerne aos serviços que se pretende atestar.

7.7.1.3.2.5. Os atestados emitidos por pessoa jurídica de direito privado devem, preferencialmente, conter assinatura digital certificada ou com reconhecimento de firma, que assegure sua autenticidade. Caso a assinatura do responsável técnico não contenha elementos de autenticação, a CONTRATANTE se resguarda ao direito de realizar diligência para solicitar documentos a fim de sanar eventuais dúvidas quanto ao referido atestado.

7.7.1.3.2.6. Tais declarações deverão ser emitidas em papel timbrado, com assinatura, identificação e telefone do emitente.

7.7.1.3.2.7. A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do (s) atestado (s).

7.7.1.3.2.8. O Tribunal de Justiça do Estado da Bahia se reserva ao direito de realizar diligências para averiguar a veracidade dos documentos e declarações junto à pessoa jurídica emissora dos Atestados e/ou Declarações, visando obter informação sobre o serviço prestado e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado

7.7.1.3.2.9. Quando solicitado através de diligência, o licitante deverá prontamente disponibilizar todas as informações necessárias à comprovação da legitimidade dos respectivos atestados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, sob pena de inabilitação.

7.7.1.3.2.10. Os atestados devem ter sido emitidos em nome da pessoa jurídica da CONTRATADA, não se admitindo atestados emitidos para pessoas físicas, ainda que sejam profissionais contratados por esta.

7.7.1.3.2.11. Todos os documentos emitidos em língua estrangeira deverão ser acompanhados da correspondente versão em português, assinada por tradutor juramentado.

7.7.1.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA, comprovada mediante apresentação de:

7.7.1.4.1. Certidão negativa de falência ou recuperação judicial, emitida pelo distribuidor da sede da pessoa jurídica, expedida nos 90 (noventa) dias anteriores à data da realização da licitação, caso o documento não consigne prazo de validade.

7.7.1.4.2. Apresentação de Balanço Patrimonial e Demonstrações Contábeis do último exercício financeiro, já exigível, na forma da lei, que comprovem a boa situação financeira da licitante podendo ser atualizada por índices oficiais na hipótese de encerrados há mais de 03 (três) meses da data de sua apresentação, vedada à substituição por Balancetes e Balanços Provisórios.

7.7.1.4.2.1. A licitante apresentará, conforme o caso, publicação no Diário Oficial ou Jornal de Grande Circulação do Balanço ou cópia reprográfica das páginas do Livro Diário numeradas sequencialmente onde foram transcritos o Balanço e a Demonstração de Resultado, com os respectivos Termos de Abertura e Encerramento registrados na Junta Comercial ou no caso de empresas sujeitas à tributação com base no lucro real, o Balanço Patrimonial e Demonstração de Resultado emitido através do Sistema Público de Escrituração Digital –SPED, contendo Recibo de Entrega do Livro, os Termos de Abertura, Encerramento e Autenticação, podendo este último ser substituído pela Etiqueta da Junta Comercial ou Órgão de Registro.

7.7.1.4.3. **Comprovação de Patrimônio Líquido**, apresentado na forma da lei, no montante correspondente a 10% (dez por cento) do valor estimado para a contratação, admitida a sua atualização com base no INPC do IBGE, permitindo-se, na hipótese de licitação por lotes, a demonstração da qualificação individualizada para o lote de interesse da proponente.

7.7.1.4.3.1. Na hipótese de licitação por lotes, o patrimônio líquido exigível será calculado em função da soma de tantos quantos forem os lotes em que a interessada tenha apresentado as melhores ofertas. Quando for atingido o limite da capacidade econômico-financeira da proponente, esta será declarada inabilitada para o(s) lote(s) subsequentes, observada a ordem sequencial dos lotes constante do instrumento convocatório, sendo vedada a escolha, pela proponente, dos lotes para os quais deseja a habilitação.

7.7.1.4.5. DECLARAÇÃO DE PROTEÇÃO AO TRABALHO DO MENOR, em atendimento ao inciso XXXIII do art. 7º da Constituição Federal, para os fins do disposto no inciso V do art. 98 da Lei Estadual nº 9.433/05, conforme modelo constante do **Anexo XIII deste Edital.**

7.7.1.4.6. O CERTIFICADO DE REGISTRO CADASTRAL - CRC, expedido pela Secretaria de Administração do Estado da Bahia/SAEB, no seu prazo de validade, poderá substituir todos os documentos relativos à habilitação, exceto os concernentes à Qualificação Técnica, condicionado à verificação da validade dos documentos cadastrais, através do sistema SIMPAS. Caso o CRC consigne algum documento vencido, o licitante deverá apresentar a versão atualizada do referido documento no envelope de habilitação.

7.7.2. Serão realizadas consultas aos seguintes cadastros:

a) Consulta Consolidada de Pessoa Jurídica (Certidão Conjunta TCU, CNJ, Portal Transparência (CEIS e CNEP) – https://certidoes-apf.apps.tcu.gov.br/);
b) Sistema de Sanções e Penalidades do Tribunal de Justiça da Bahia;
c) Fornecedores com Penalidades (www.comprasnet.ba.gov.br).

7.7.3. Regras acerca da participação de matriz e filial

a) se o licitante for a matriz da empresa, todos os documentos devem estar em nome da matriz;

b) se o licitante for filial, todos os documentos devem estar em nome da filial, dispensada a apresentação dos documentos que, pela própria natureza, comprovadamente sejam emitidos somente em nome da matriz;

c) os atestados de capacidade técnica/responsabilidade técnica, quando exigidos, podem ser apresentados em nome e com CNPJ da matriz e/ou da filial da empresa licitante;

d) Se a licitante participar do certame apresentando os documentos de habilitação da matriz e desejar executar o contrato pela filial, ou vice-versa, deverá fazer prova, por ocasião da assinatura do contrato, da regularidade do estabelecimento que executará o objeto licitado, a qual deverá ser mantida durante todo o curso da avença.

7.7.4. Os documentos de habilitação deverão ser apresentados conforme o disposto no item 7.7.deste Edital.

8. DA ABERTURA DA SESSÃO PÚBLICA

8.1. A qualquer tempo, antes da data fixada para apresentação das propostas, poderá o Pregoeiro, se necessário, modificar este Edital, hipótese em que deverá proceder a divulgação, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

8.1.1 As modificações do edital serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes. [NOTA: art. 15 do Decreto no 19.896/20]

8.2. A licitante poderá retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema eletrônico, até a data e o horário estabelecidos no edital para a sua apresentação. [NOTA: art. 18, §6o, do Decreto no 19.896/20].

8.3. A partir do horário previsto neste edital, a sessão pública *na internet* será aberta pelo pregoeiro com a utilização de sua chave de acesso e senha. [NOTA: art. 19, caput, do Decreto no 19.896/20]

8.3.1 As licitantes poderão participar da sessão pública na internet, mediante a utilização de sua chave de acesso e senha. [NOTA: art. 19, §1o, do Decreto no 19.896/20]

8.4. Iniciada a sessão pública do Pregão Eletrônico, não cabe desistência da proposta. [NOTA: art 19, §1º do Decreto Estadual nº 19.896/2020 e Decreto Judiciário nº 44/2003].

8.5. O pregoeiro verificará as propostas apresentadas e desclassificará aquelas que não estejam em conformidade com os requisitos estabelecidos neste edital. [NOTA: art. 20, caput, do Decreto nº 19.896/20]

8.5.1. Serão consideradas irregulares e desclassificadas, de logo, as propostas que não contenham informação que permita a identificação do objeto proposto.

8.5.1.1 Também será desclassificada a proposta que identifique a licitante.

8.5.2. A desclassificação da proposta será fundamentada e registrada no sistema eletrônico, para acompanhamento por todos os participantes. [NOTA: art. 20, parágrafo único, do Decreto no 19.896/20]

8.5.3. O sistema eletrônico ordenará automaticamente as propostas classificadas pelo pregoeiro. [NOTA: art. 21, caput, do Decreto no 19.896/20]

8.5.4. Somente as propostas classificadas pelo pregoeiro participarão da etapa de envio de lances. [NOTA: art. 21, parágrafo único, do Decreto no 19.896/20]

8.6. Havendo apenas uma oferta, esta poderá ser aceita, desde que atenda todas as condições do instrumento convocatório e seu preço seja compatível com o valor estimado para a contratação e dentro da realidade do mercado.

8.7. O sistema eletrônico disponibilizará campo próprio para troca de mensagens entre o pregoeiro e as licitantes. **[NOTA: art. 19, §2º, do Decreto nº 19.896/20]**

9. ETAPA COMPETITIVA DE LANCES ELETRÔNICOS, MODO DE DISPUTA E JULGAMENTO DAS PROPOSTAS

DOS LANCES ELETRÔNICOS

9.1. Classificadas as propostas, o pregoeiro dará início à fase competitiva, oportunidade em que os licitantes poderão encaminhar **lances exclusivamente por meio do sistema eletrônico**. [NOTA: art. 22 do Decreto no 19.896/20]

9.1.1 É vedada a utilização de sistema robotizado que implique envio automático de lances.

9.1.1.1. Poderá ser fixado intervalo mínimo de tempo a ser observado entre as ofertas de lances, ou recurso de tecnologia disponibilizado pelo sistema, a fim de coibir a utilização de software lançador (robô).

9.1.2 Se o pregoeiro identificar que algum licitante, ao apresentar seus lances, o fez, entre outras formas, de maneira sucessiva, padronizada, intermitente, simultânea ou em intervalos de poucos segundos entre eles, indicando a utilização de software lançador "robô", será ela desclassificada, com a consequente abertura de processo administrativo para apuração do ilícito.

9.1.3 A licitante será imediatamente informada do recebimento do lance e do valor consignado no registro. [NOTA: art. 22, §1o, do Decreto no 19.896/20]

9.1.4 As licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão pública e as regras estabelecidas neste edital. [NOTA: art. 22, §2o, do Decreto no 19.896/20]

9.1.5 A licitante somente poderá oferecer valor inferior ou maior percentual de desconto ao último lance por ela ofertado e registrado pelo sistema, observado, quando houver, o intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta. [NOTA: art. 22, §3o, do Decreto no 19.896/20]

9.1.6 Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro. [NOTA: art. 22, §4o, do Decreto no 19.896/20]

9.1.7 Durante a sessão pública, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, **vedada a identificação da licitante**. [NOTA: art. 22, §5o, do Decreto no 19.896/20]

DO ENVIO DE LANCES

9.2. **A etapa de lances dar-se-á por meio do modo de disputa aberto** e será observado o seguinte procedimento:

a) as licitantes apresentarão lances públicos e sucessivos, com prorrogações, conforme o critério de julgamento adotado neste edital;
b) deverá ser observado o intervalo mínimo de diferença de valores ou de percentuais entre os lances, definido neste edital, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta;
c) a etapa de envio de lances na sessão pública durará 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública. [NOTA: art. 23, caput, do Decreto no 19.896/20]
d) a prorrogação automática da etapa de envio de lances, de que trata a letra "c" será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários. [NOTA: art. 23, §1o, do Decreto no 19.896/20]
e) na hipótese de não haver novos lances, a sessão pública será encerrada automaticamente. [NOTA: art. 23, §2o, do Decreto no 19.896/20]
f) encerrada a sessão pública sem prorrogação automática pelo sistema, nos termos do disposto no § 1º deste artigo na letra "d", o pregoeiro poderá admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço, mediante justificativa. [NOTA: art. 23, §3o, do Decreto no 19.896/20]

DA INTERRUPÇÃO DA SESSÃO

9.3. Sempre que houver interrupção da sessão, as licitantes deverão ser notificadas do dia e hora em que a sessão terá continuidade.

9.3.1 Na hipótese de o sistema eletrônico desconectar para o pregoeiro no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados. [NOTA: art. 25 do Decreto no 19.896/20]

9.3.2 Na situação descrita no item 9.3.1, quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes, no sítio eletrônico utilizado para divulgação. [NOTA: art. 26 do Decreto no 19.896/20]

DOS CRITÉRIOS DE DESEMPATE

9.4 Em caso de empate, real ou ficto, será assegurada, nos termos dos arts. 44 e 45 da Lei complementar no 123/06, a preferência de contratação para as microempresas e empresas de pequeno porte beneficiárias do regime diferenciado e favorecido, nos termos que se seguem:

9.4.1. Entende-se por empate ficto as situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam até 5% (cinco por cento) superiores à proposta mais bem classificada, e empate real as que sejam iguais.
9.4.2. Em qualquer das hipóteses de empate, a microempresa ou empresa de pequeno porte mais bem classificada poderá apresentar, no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, proposta de preço inferior àquela de menor valor exequível, sob pena de preclusão.
9.4.3. Se a microempresa ou empresa de pequeno porte mais bem classificada não exercer o direito, ou se sua oferta não for aceita, ou se for inabilitada, será concedido idêntico direito à microempresa ou empresa de pequeno porte subsequente em situação de empate, se houver, na ordem classificatória, até a apuração de uma proposta que atenda às condições estabelecidas no edital.
9.4.4. No caso de as microempresas e empresas de pequeno porte apresentarem preços iguais, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
9.4.5. **O disposto neste item somente se aplica quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte.**
9.4.6. Se não ocorrer o desempate, prevalecerá a melhor oferta inicial.
9.4.7. Se a melhor oferta não puder ser aceita, ou se for inabilitada a sua proponente, o responsável pela licitação avaliará a proposta subsequente, procedendo a nova verificação da ocorrência do empate ficto, se for o caso, de acordo com a disciplina ora estabelecida, e assim sucessivamente, até a obtenção de proposta válida.
9.4.8. Ocorrendo empate de propostas formuladas por licitantes que não detenham a condição de microempresa ou de empresa de pequeno porte, será observado o disposto no art. 92 da Lei estadual nº 9.433/05, procedendo-se, sucessivamente, a sorteio em ato público, para o qual as licitantes serão convocadas, vedado qualquer outro critério.
9.4.9. No caso de empate real entre as propostas apresentadas por microempresas e empresas de pequeno porte, em razão da ausência de disputa de lances, será realizado sorteio em ato público, para o qual as licitantes serão convocadas.
9.4.10. Sempre que houver sorteio deverá ser lavrada ata específica.

9.5. Em se tratando de licitações exclusivas para microempresa e empresa de pequeno porte, e no caso de empate real entre as propostas apresentadas por microempresas e empresas de pequeno porte, será realizado sorteio em ato público, para o qual as licitantes serão convocadas.

9.5.1. Sempre que houver sorteio deverá ser lavrada ata específica.

9.6. Os critérios de desempate serão aplicados nos termos do item 9.4 ou 9.5, conforme o caso, se não houver envio de lances após o início da fase competitiva.

BENEFÍCIO ÀS MICROEMPRESAS (ME) E EMPRESAS DE PEQUENO PORTE (EPP) - DA REGULARIZAÇÃO FISCAL E TRABALHISTA DAS ME E EPP

9.7. A existência de restrição na comprovação da regularidade fiscal e trabalhista das microempresas e empresas de pequeno porte sujeitas ao regime da Lei Complementar nº 123/06, alterada pela Lei Complementar nº147/2014, não implica na inabilitação automática da licitante em face do disposto no art. 42 deste diploma, devendo ser realizada a **habilitação com ressalva de existência de restrição fiscal e trabalhista e trabalhista** e diferindo-se a comprovação da regularidade na forma deste edital.

9.7.1. Sagrando-se vencedora do certame microempresa ou empresa de pequeno porte, beneficiária do regime diferenciado da Lei Complementar no 123/06, cuja habilitação tenha sido procedida com a ressalva de existência de restrição fiscal e/ou trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada a vencedora do certame, prorrogável por igual período, a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

9.7.2. A não-regularização da documentação no prazo previsto neste item implicará decadência do direito à contratação, sem prejuízo das sanções previstas pelo ilícito tipificado no art. 184, VI da Lei estadual no 9.433/05, sendo facultado à Comissão de Licitação ou ao pregoeiro, conforme o caso, proceder à convocação das licitantes remanescentes, na ordem de classificação, ou revogar a licitação.

DA DIVULGAÇÃO DO ORÇAMENTO

9.8. Na hipótese de a licitação se processar com o orçamento sigiloso, o valor estimado ou o valor máximo aceitável para a contratação, bem como os elementos de sua composição, serão tornados públicos apenas e imediatamente após o encerramento do envio de lances. **[NOTA: art. 7o, §4o, do Decreto no 19.896/20]**

DA NEGOCIAÇÃO DA PROPOSTA COMERCIAL

9.9. Encerrada a etapa de envio de lances da sessão pública, o **pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta à licitante** que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas no edital. [NOTA: art. 28, caput, do Decreto no 19.896/20]

9.9.1 A negociação será realizada por meio do sistema eletrônico e poderá ser acompanhada pelos demais licitantes. [NOTA: art. 28, §1o, do Decreto no 19.896/20]

ADEQUAÇÃO DA PROPOSTA COMERCIAL

9.10. O pregoeiro concederá o prazo de três horas para envio da proposta escrita adequada ao último lance ofertado após a negociação de que trata o item 9.9 acima, podendo ser prorrogado, mediante justificativa. **[NOTA: art. 28, §2o, do Decreto no 19.896/20] [NOTA: art. 33 do Decreto no 19.896/20]**

9.10.1 A nova proposta deverá contemplar a planilha com os respectivos valores readequados ao valor ofertado e registrado de menor lance, durante a fase de lances.

9.10.1.1 Na hipótese de contratação de serviços comuns em que a legislação ou o edital exija apresentação de planilha de composição de preços, esta deverá ser encaminhada exclusivamente via sistema eletrônico, no prazo do item 9.10 acima com os respectivos valores readequados ao lance vencedor. [NOTA: art. 30, §5o, do Decreto no 19.896/20

9.10.2. Os documentos deverão ser apresentados em formato digital, via sistema.

9.10.3. Caso seja necessário, o pregoeiro poderá solicitar documentos complementares à proposta, a fim de esclarecer ou confirmar situação fática ou jurídica pré-existente, os quais deverão ser apresentados em formato digital, via sistema, no prazo de três horas a contar da solicitação, sendo vedada a inclusão de elemento que devesse constar originariamente da proposta. **[NOTA: art. 30, §3o, do Decreto no 19.896/20]**

9.10.3.1. A vedação à inclusão de novo documento, prevista no art. 30, §3º do Decreto Estadual nº 19.896/2020, bem como no art. 43, §3º da Lei Federal nº 8.666/93, não alcança documento destinado a atestar condição de habilitação preexistente à abertura da sessão pública, apresentado em sede de diligência (Acórdão 1211, 2443 e 2568, todos expedidos em 2021 pelo Plenário do TCU).

9.11. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação. **[NOTA: art. 29 do Decreto nº 19.896/20]**

DA COMPATIBILIDADE DO PREÇO

9.12. Será desclassificada a proposta que consignar valor global superior aos praticados no mercado ou, quando for o caso, que contemple preços superiores aos preços máximos definidos no instrumento convocatório, fixados pela Administração ou por órgão oficial competente ou, ainda, aos constantes do sistema de registro de preços.

9.12.1. Somente serão admitidas propostas com valores unitários e totais que estejam dentro dos limites máximos estimados pelo TJBA.

9.12.1.1. Os critérios de aceitabilidade de valores são cumulativos, verificando-se a adequação da oferta tanto em relação aos valores totais/globais quanto aos valores unitários estimativos da licitação.

9.12.2. Serão também desclassificadas as propostas que consignarem preços manifestamente inexequíveis, assim considerados aqueles que não venham a ter demonstrada sua viabilidade através de documentação que comprove **que os custos dos insumos são coerentes com os de mercado** e que os coeficientes de produtividade são compatíveis com a execução do objeto do contrato.

9.12.3. Caso seja verificada pelo(a) Pregoeiro(a), na proposta de preços apresentada, a ocorrência de erro formal ou material sanável que não impacte em majoração do valor global ofertado, poderá ser concedido um prazo, definido pelo(a) pregoeiro(a), para a licitante realizar os devidos ajustes, com consequente reenvio da proposta de preços em sistema.

9.13. Se a melhor oferta não puder ser aceita, o responsável pela licitação avaliará a proposta subsequente, procedendo a nova verificação da ocorrência do empate ficto, se for o caso, observando o mesmo rito estabelecido, e assim sucessivamente, até a obtenção de proposta válida.

10. DO JULGAMENTO DA HABILITAÇÃO

10.1. O pregoeiro conferirá e examinará os documentos de habilitação, emitindo o Certificado de Registro das empresas cadastradas e verificando a regularidade da documentação exigida no instrumento convocatório. [NOTA: art. 30, caput, do Decreto no 19.896/20]

10.1.1 Serão inabilitadas as licitantes cujos documentos exigidos para habilitação não tenham sido apresentados na forma do edital, ou que não estejam contemplados no Registro Cadastral, ou que dele constem como vencidos, ressalvado o disposto no item 10.1.2. [NOTA: art. 30, §1o, do Decreto no 19.896/20]

10.1.2 Desde que possível tecnicamente, a verificação pelo órgão ou entidade promotora do certame nos sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação. [NOTA: art. 30, §2o, do Decreto no 19.896/20]

10.1.3 Caso seja necessário, o pregoeiro poderá solicitar documentos complementares à habilitação, a fim de esclarecer ou confirmar situação fática ou jurídica pré-existente, os quais deverão ser apresentados em formato digital, via sistema eletrônico, no prazo de 03 (três) horas a contar da solicitação, vedada a inclusão posterior de elemento que devesse constar originariamente dos documentos de habilitação. [NOTA: art. 30, §3o do Decreto no 19.896/20]

10.1.4. A documentação poderá ser encaminhada, a critério do(a) Pregoeiro(a), para validação por área(s) técnica(s) competente(s) do TJBA, a(s) qual(is) emitirá(ão) parecer conclusivo que orientará a decisão do(a) Pregoeiro(a) para fins de habilitação/inabilitação de licitante.

10.2. Não sendo aceitável a proposta vencedora, ou se o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital. [NOTA: art. 30, §4o, do Decreto no 19.896/20]

10.3. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte será exigida nos termos do disposto nos arts. 42 e 43, ambos da Lei Complementar Federal nº 123, de 14 de dezembro de 2006. [NOTA: art. 30, §6o do Decreto no 19.896/20]

10.4. Constatado o atendimento às exigências estabelecidas no edital, a licitante será declarada vencedora. [NOTA: art. 30, §7o do Decreto no 19.896/20]

10.4.1 Havendo necessidade de suspensão da sessão pública para a declaração do vencedor por prazo superior a 03 (três) horas a contar do encerramento da etapa de lances, a nova sessão somente poderá ser reiniciada mediante aviso prévio no sistema eletrônico, observada a antecedência mínima de 24 (vinte e quatro) horas, e a ocorrência será registrada em ata. [NOTA: art. 30, §8o do Decreto no 19.896/20]

11. DO SANEAMENTO DA PROPOSTA E DA HABILITAÇÃO

11.1. O pregoeiro poderá em qualquer fase da licitação, suspender os trabalhos, procedendo ao registro da suspensão e a convocação para a continuidade dos mesmos, bem como promover diligências destinadas a esclarecer ou a complementar a instrução do processo licitatório, desde que não implique em inclusão de documento ou informação que deveria constar originariamente da proposta.

11.1.1. A vedação à inclusão de novo documento, prevista no art. 30, §3º do Decreto Estadual nº 19.896/2020, bem como no art. 43, §3º da Lei Federal nº 8.666/93, não alcança documento destinado a atestar condição de habilitação preexistente à abertura da sessão pública, apresentado em sede de diligência (Acórdão 1211, 2443 e 2568, todos expedidos em 2021 pelo Plenário do TCU).

11.2. O pregoeiro poderá, no julgamento da habilitação e das propostas, sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação e classificação. [NOTA: art. 31, caput, do Decreto no 19.898/20]

11.2.1 Havendo necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata este item, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata. [NOTA: art. 31, §1o, do Decreto no 19.898/20]

11.2.2 Quando todas as propostas forem desclassificadas ou todos os licitantes forem inabilitados, o pregoeiro poderá, caso se esta funcionalidade estiver disponível no sistema, suspender o pregão e estabelecer uma nova data, com prazo não superior a 03 (três) dias úteis, para o recebimento de nova proposta ou nova documentação, após sanadas as causas que motivaram a desclassificação ou inabilitação. [NOTA: art. 31, §2o, do Decreto no 19.898/20]

11.3. O pregoeiro poderá, a qualquer tempo, negociar com o proponente da melhor oferta aceitável, visando obter preço menor.

12. RECURSOS DIRIGIDOS AO PREGOEIRO

12.1. Declarado o vencedor, qualquer licitante poderá, **no prazo de até 30 (trinta) minutos** manifestar sua intenção de recorrer, de forma imediata e motivada, em campo próprio do sistema eletrônico. [NOTA: art. 32 do Decreto no 19.896/20]

12.1.1. Caso não seja declarado o vencedor da disputa imediatamente após o encerramento da sessão, o Pregoeiro divulgará, no sistema eletrônico, a data e horário em que será feita a proclamação declaratória do vencedor, para que seja iniciado o prazo recursal.

12.2. As razões do recurso de que trata o caput deste artigo deverão ser apresentadas no prazo de **03 (três) dias úteis**, ficando as demais licitantes intimadas para, se desejarem, apresentar suas contrarrazões, em igual prazo, contado a partir do primeiro dia útil subsequente ao da data final do prazo do recorrente, assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses, na 5ª Av. do CAB (Centro Administrativo da Bahia – CAB), Edifício-Sede do Tribunal de Justiça do Estado da Bahia, nº 560, 1º andar, sala 119-norte, NCL, Salvador-Bahia CEP 41.746-970. [NOTA: art. 32, §§1º e 2º do Decreto no 19.896/20].

12.3. Os recursos e contrarrazões deverão ser dirigidas a(o) pregoeiro(a) responsável pela condução do certame, e encaminhadas através de campo próprio no sistema de licitação, **até as 23:59h** do último dia do prazo.

12.4. A ausência de manifestação imediata e motivada da licitante quanto à intenção de recorrer, nos termos do disposto no caput deste artigo, importará na decadência desse direito, e o pregoeiro estará autorizado a adjudicar o objeto à licitante declarada vencedora. [NOTA: art. 32, §3o, do Decreto no 19.896/20]

12.5. O acolhimento do recurso importará na invalidação apenas dos atos que não podem ser aproveitados. [NOTA: art. 32, §4o, do Decreto no 19.896/20]

13. ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade superior fará a adjudicação do objeto ao licitante vencedor e homologará a licitação. [NOTA: art. 34, caput, do Decreto no 19.896/20]

13.2. Na ausência de recurso ou quando a decisão que o ensejou tenha sido reconsiderada, caberá ao pregoeiro adjudicar o objeto, encaminhar o processo devidamente instruído à autoridade superior e propor a homologação. [NOTA: art. 34, parágrafo único, do Decreto no 19.896/20]

13.3. A homologação e adjudicação do objeto desta licitação não implicarão direito à contratação.

13.4. Após a homologação, o Tribunal de Justiça do Estado da Bahia convocará a licitante vencedora para assinatura do instrumento de contrato, nos termos do **Anexo X – MINUTA DE CONTRATO**, através de seu representante legal ou outro mandatário com poderes expressos.

14. CONTRATAÇÃO

14.1. Como condição para celebração do contrato, a licitante vencedora deverá fazer prova da manutenção de todas as condições de habilitação, o que também poderá ser aferido, se disponível, mediante consulta ao Registro Cadastral ou a sites oficiais.

14.2. A contratação com a licitante vencedora obedecerá às condições da minuta de contrato constante do instrumento convocatório, facultada a substituição, a critério da Administração, por instrumento equivalente, desde que presentes as condições do art. 132 da Lei estadual no 9.433/05.

14.2.1. Considerar-se-ão literalmente transcritas no instrumento equivalente todas as cláusulas e condições previstas na minuta de contrato constante do convocatório.

14.3. O adjudicatário será convocado a assinar o termo de contrato, ou instrumento equivalente, se for o caso, no prazo de 05 (cinco) dias, na forma dos §§3o e 4o do art. 124 da Lei estadual no 9.433/05, a contar da sua notificação, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no inciso I do art. 192 e no art. 194 da Lei estadual no 9.433/05, podendo solicitar sua prorrogação por igual período, por motivo justo e aceito pela Administração.

14.3.1 A assinatura do contrato, ou instrumento equivalente, se for o caso, deverá ser realizada pelo representante legal da empresa ou mandatário com poderes expressos.

14.3.2. A recusa injustificada do fornecedor em subscrever o termo de contrato ou instrumento equivalente ensejará a aplicação das penalidades legalmente estabelecidas. [NOTA: conforme §1o do art. 36 do Decreto no 19.896/20]

14.3.3 Equipara-se à recusa prevista no item 14.3.3 a circunstância de o fornecedor deixar de manter as condições de habilitação exigidas na licitação, ou, por qualquer meio, dar causa à impossibilidade de subscrição do contrato. [NOTA: conforme §2o do art. 36 do Decreto no 19.896/20]

14.4. Na hipótese de o licitante vencedor, convocado dentro do prazo de validade de sua proposta, não assinar o Termo de Contrato ou não aceitar ou retirar o instrumento equivalente, é facultado ao pregoeiro examinar e verificar a aceitabilidade das propostas subsequentes, na ordem de classificação, bem como o atendimento das condições de habilitação, adotando os procedimentos imediatamente posteriores ao encerramento da etapa de lances, sem prejuízo da aplicação das sanções previstas na legislação pertinente. **[NOTA: art. 119, parágrafo único e art. 120, XXIX da Lei estadual nº 9.433/05]**

14.5. Não serão contratados os adjudicatários que estejam com documentação irregular no Cadastro Unificado de Fornecedores do Estado da Bahia, mantido pela Secretaria de Administração do Estado da Bahia ou no Cadastro de Fornecedores do Poder Judiciário do Estado da Bahia.

14.6. VIGÊNCIA CONTRATUAL: O prazo de vigência do contrato será de 24 (vinte e quatro) meses, a partir da data da sua assinatura, prorrogáveis nos termos do Art. 140 da Lei Estadual nº 9.433/2005.

14.7. Das alterações contratuais: A **CONTRATADA** ficará obrigada a aceitar nas mesmas condições contratuais, acréscimos ou supressões que se fizerem no objeto, até **25% (vinte e cinco por cento)** do valor inicial atualizado do contrato, na forma do §1º do art. 143 da Lei Estadual nº 9.433/05.

14.7.1. Nenhum acréscimo ou supressão poderá ser realizado sem a devida motivação ou exceder o limite estabelecido no subitem anterior, salvo as supressões resultantes de acordo celebrado entre os contratantes.
14.7.2. A variação do valor contratual para fazer face ao reajuste de preços previsto no próprio contrato, quando for o caso, as atualizações, compensações ou apenações financeiras decorrentes das condições de pagamento nele previstas, bem como o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido, não caracterizam alteração do mesmo, podendo ser registrados por simples apostila, dispensando a celebração de aditamento.

14.8. Da subcontratação e do consórcio: Não serão admitidas a subcontratação do objeto licitado e a participação de interessados sob a forma de consórcio.

14.8.1. Será admitida, caso necessário, a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que: sejam observados, pela nova pessoa jurídica, todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado; e haja a anuência expressa da Administração à continuidade do contrato.

14.9. Da Garantia Contratual: Em face ao risco econômico da contratação, em garantia de plena, fiel e segura execução de tudo o que se há obrigado, a CONTRATADA prestará garantia de **5% (cinco por cento)** sobre o preço global do objeto a ser contratado, devendo apresentar comprovante de sua prestação, no prazo máximo de **10 (dez) dias corridos**, contados da data da assinatura do contrato, devendo, ainda, ser atualizada periodicamente.

14.9.1. A garantia será prestada em caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, pelo prazo equivalente ao deste contrato acrescido de mais 03 (três) meses do término da vigência contratual, devendo ser renovada a cada prorrogação.

14.9.2. A garantia em dinheiro deverá ser efetuada no Banco do Brasil, com correção monetária, em favor da CONTRATANTE. O cálculo da atualização monetária do valor caucionado em dinheiro será feito aplicando-se o índice mais vantajoso para a Administração entre a data de retenção da caução e da devolução do seu valor.

14.9.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas; e/ou
b) prejuízos causados à administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do

contrato; e/ou
c) as multas moratórias e punitivas aplicadas pela Administração à CONTRATADA; e/ou
d) obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela CONTRATADA.

14.9.4. Não serão aceitas garantias em cujos termos não constem expressamente os eventos indicados nas alíneas **'a'** a '**d'** do item 14.9.3.

14.9.5. O garantidor deverá declarar expressamente que tem plena ciência dos termos do edital e das cláusulas contratuais.

14.9.6. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Tribunal de Justiça da Bahia com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

14.9.7. A CONTRATANTE não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:
a) caso fortuito ou força maior;
b) alteração, sem prévia anuência da seguradora ou do fiador, das obrigações contratuais;
c) descumprimento das obrigações pelo contratado decorrentes de atos ou fatos praticados pela Administração;
d) atos ilícitos dolosos praticados por servidores da Administração.

14.9.8. Cabe à própria administração apurar a isenção da responsabilidade prevista nas alíneas **'c'** e **'d'** do item 14.9.7. acima, não sendo a entidade garantidora parte no processo instaurado pela CONTRATANTE.

14.9.9. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas no item 14.9.7.

14.9.10. A garantia será considerada extinta após a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

14.9.11. A garantia será obrigatoriamente revista e complementada quando houver redução da sua representatividade percentual por variação econômica do contrato ou descontos de valores devidos à CONTRATANTE.

14.9.12. A liberação da garantia ou sua restituição se dará após o recebimento definitivo do objeto do contrato ou da comprovação de quitação de todas as obrigações trabalhistas e previdenciárias dos recursos humanos envolvidos na execução contratual, inclusive garantidas eventuais demandas judiciais decorrentes da presente contratação, nos termos do Instrumento Contratual, e quando em dinheiro, atualizada monetariamente, deduzidos eventuais valores devidos à CONTRATANTE.

14.9.13. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

14.9.14. O valor da garantia permanecerá integral até o término da vigência do Contrato. Se o valor da garantia for utilizado, total ou parcialmente, pela CONTRATANTE, para compensação de prejuízo causado no decorrer da execução contratual por conduta da CONTRATADA, esta deverá proceder à respectiva reposição **no prazo de 10 (dez) dias corridos**, contados da data em que tiver sido notificada.

14.9.15. A garantia responderá pelo inadimplemento das obrigações contratuais e multas impostas, independentemente de outras cominações legais.

15. CONDIÇÕES DE PAGAMENTO

15.1. DO PAGAMENTO

15.1.1. O faturamento só poderá ser apresentado após a emissão do Termo de Recebimento Definitivo (TRD), indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao fornecimento e prestação dos serviços, acompanhado da documentação probatória relativa ao recolhimento dos impostos relacionados com a obrigação, obedecidos os prazos descritos no item **3.3.1 – Cronograma de Entrega dos Serviços do Anexo I – Termo de Referência.**.

15.1.2. Devido à política global de venda do fabricante, para os itens de 01 a 05, componentes da solução, o pagamento será efetuado em parcela única após Termo de Recebimento Definitivo a ser emitido para cada um dos itens.

15.1.3. Para o item 06 da solução, que ocorrerá sob demanda, o faturamento também será feito em parcela única, de acordo com o consumo, e só poderá ser apresentado após a CONTRATANTE emitir o TRD do respectivo item, indicando a realização e satisfação com os treinamentos entregues;

15.1.4. Para o item 07 da solução, o pagamento será realizado mensalmente, após verificados os critérios descritos nos itens 3.5 (Acompanhamento dos Prazos de Garantia e Níveis Mínimos de Serviço) e 3.6 (Instrumentos de Medição dos Serviços), ambos do Anexo I – Termo de Referência. Deverá ser apresentada uma Nota Fiscal para cada mês de serviço prestado.

15.1.5. Os faturamentos deverão ser apresentados **em notas fiscais de venda ou serviço**, de acordo com as características de cada objeto, e serão pagos por meio de ordem bancária ou crédito em conta corrente, em até 08 (oito) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, condicionado ao seu ateste pelo Gestor do Contrato, em consonância com o disposto no art. 6º, § 5º; art. 8º, XXXIV; art. 79, XI, "a"; art. 154, V e art. 155, V da Lei Estadual nº 9.433/05.

15.1.6. O valor global a ser pago à CONTRATADA deverá atender aos valores cotados na proposta vencedora.

15.1.7. A efetivação e aceite de quaisquer serviços não previstos só poderão ocorrer mediante aprovação formal do CONTRATANTE.

15.1.8. Na ocasião de ocorrência de erro na(s) nota(s) fiscal(s)/fatura(s) ou qualquer circunstância que impeça a liquidação da despesa, aquela será restituída ou será comunicada a irregularidade à CONTRATADA, ficando pendente de pagamento até que esta providencie as medidas saneadoras. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação e/ou a reapresentação do documento fiscal, não acarretando qualquer ônus para a CONTRATANTE;

15.1.9. A CONTRATANTE poderá deduzir do montante a pagar ou do montante depositado como garantia, quando for o caso, valores correspondentes a multas ou indenizações devidas pela CONTRATADA, decorrentes de penalidades aplicadas nos termos do Contrato e deste Termo de Referência;

15.1.10. Em hipótese alguma serão pagos serviços não contratados;

15.1.11. A CONTRATADA deverá apresentar nota fiscal correspondente ao objeto fornecido, reservando-se o CONTRATANTE o direito de não atestá-la para o pagamento se os dados nela constantes estiverem em desacordo com as especificações apresentadas neste Edital, ficando o pagamento suspenso até a regularização.

15.1.12. O atesto na nota fiscal é condição indispensável para o pagamento desta. Na ausência do gestor, o atesto será dado por gestor substituto.

15.1.13. O CNPJ constante da nota fiscal deverá ser o mesmo indicado na proposta, nota de empenho e vinculado à conta-corrente da CONTRATADA.

15.1.14. A CONTRATADA deverá obedecer integralmente às disposições quanto à obrigatoriedade de emissão da Nota Fiscal por meio eletrônico, nos termos do Regulamento do ICMS Bahia, com as alterações contidas no Decreto Estadual nº 10.666 de 03/08/2006.

16. MANUTENÇÃO DOS PREÇOS, REAJUSTAMENTO E REPACTUAÇÃO

16.1. Os preços são fixos e irreajustáveis durante a vigência inicial do contrato.

16.2. Dentro do prazo de vigência, em caso de prorrogação do contrato mediante solicitação da CONTRATANTE, os valores contratados poderão ser reajustados, aplicando o ICTI (Índice de Custos de Tecnologia da Informação). Caso o índice estabelecido para reajuste venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação vigente.

17. DA FISCALIZAÇÃO DO CONTRATO E DO RECEBIMENTO DO OBJETO

17.1. Competirá ao CONTRATANTE proceder ao acompanhamento da execução do contrato, na forma do art. 154 da Lei estadual 9.433/05, ficando esclarecido que a ação ou omissão, total ou parcial, da fiscalização do CONTRATANTE não eximirá a CONTRATADA de total responsabilidade na execução do contrato.

17.2. O adimplemento da obrigação contratual por parte da CONTRATADA ocorre com a efetiva prestação do serviço, a realização da obra, a entrega do bem, assim como qualquer outro evento contratual cuja ocorrência esteja vinculada à emissão de documento de cobrança, consoante o art. 8º, inc. XXXIV, da Lei estadual 9.433/05.

17.3. Cumprida a obrigação pela CONTRATADA, caberá ao CONTRATANTE proceder ao recebimento do objeto, a fim de aferir se os serviços ou fornecimentos foram efetuados, para efeito de emissão da habilitação de pagamento, conforme o art. 154, inc. V, e art. 155, inc. V, da Lei estadual 9.433/05.

17.4. **A emissão de aceite dos serviços pelo CONTRATANTE não exime a CONTRATADA da responsabilidade pela correção de erros porventura identificados, sem ônus adicional, durante a execução dos serviços e vigência contratual, conforme disposto no Art. 157 da Lei 9.433/2005. Surgindo deficiências durante a execução dos serviços e vigência contratual, o CONTRATANTE requererá, por escrito, a resolução dos problemas, ficando a CONTRATADA obrigada a providenciar, junto ao fabricante, a recomposição do nível de serviços condizente com as exigências desta contratação.**

17.5. O TJBA designará servidor responsável para realizar o recebimento dos objetos, da seguinte forma:

17.5.1. TERMO DE RECEBIMENTO PROVISÓRIO: Para os itens de hardware: Deverão ser comprovadas as entregas desses objetos nas dependências do TJBA, no prazo definido no **item 3.3.1 - cronograma de entrega dos serviços do Anexo I – Termo de Referência deste Edital**.

17.5.1.1. Todas as comprovações serão aceitas em formato digital ou impresso, via *e-mail* ou presencialmente.

17.5.2. TERMO DE RECEBIMENTO DEFINITIVO: Os Termos de Recebimento Definitivo serão emitidos conforme a seguir:

a) Para os itens de *Software*: Os objetos deverão ser entregues através de carta emitida pelo fabricante, contendo as informações dos objetos contratados, o regime de suporte especificado no termo de referência, os dados de acesso do TJBA ao portal de suporte do fabricante, a vigência dos serviços contratados, os dados do cliente e do fabricante, e o registro informativo de que os produtos foram adquiridos através do licitante arrematante.
b) Para os itens de *Hardware*: Os objetos deverão ser instalados fisicamente no *Datacenter*, na sede do TJBA.
c) Para os itens de treinamento: Será atestado o recebimento dos itens em até 10 (dez) dias corridos, após a realização dos treinamentos previstos nesta contratação.
d) Para os itens de prestação de serviços: Serão emitidos mensalmente, após cumpridos os requisitos descritos nos itens 3.5 (Acompanhamento dos Prazos de Garantia e Níveis Mínimos de Serviço), 3.6 (Instrumentos de Medição dos Serviços) e seus subitens, constantes do Anexo I – Termo de Referência.

17.5.2.1. Os **Termos de Recebimento Definitivo**, nos termos do Art. 161 da Lei Estadual nº 9.433/2005, serão emitidos em razão de parecer circunstanciado de servidor ou comissão designada pela autoridade competente, mediante termo assinado pelas partes, após as entregas das atividades descritas neste item, nos prazos indicados no item 3.3.1. – Cronograma de Entrega dos Serviços do Anexo I – Termo de Referência deste Edital, sendo observado o disposto no art. 157 da mesma Lei.

17.5.2.2. A emissão de aceite dos serviços pelo CONTRATANTE não exime a CONTRATADA da responsabilidade pela correção de erros porventura identificados, sem ônus adicional.

17.6. Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar as nota(s) fiscal (is)/fatura(s) para pagamento.

17.7. A administração indicará servidores (fiscal e suplente), por meio de portaria devidamente publicada, para acompanhar o presente objeto deste certame.

17.8. Os serviços prestados serão gerenciados e fiscalizados por representantes do CONTRATANTE, que poderão exigir da CONTRATADA, a qualquer tempo, esclarecimentos, demonstrações e documentos que comprovem a regularidade do contrato.

17.9. A ação ou omissão total ou parcial da fiscalização por parte do **CONTRATANTE**, não eximirá a **CONTRATADA** da total responsabilidade na execução dos serviços objeto do presente contrato.

18. DOS ILÍCITOS E PENALIDADES

18.1. Licitantes e contratadas cumprirão, rigorosamente as condições estabelecidas neste edital, seus anexos e na proposta vencedora, para a participação neste certame e fornecimento do objeto desta licitação, inclusive obrigações adicionais estabelecidas neste edital.

18.2. As sanções serão aplicadas levando-se em conta a natureza e a gravidade da falta, os prejuízos advindos para a Administração Pública e a reincidência na prática do ato, após regular processo administrativo, desde que assegurado o direito de defesa.

18.3. Constituem ilícitos administrativos as condutas previstas nos arts. 184 e 185, da Lei nº 9.433/05, sujeitando-se os infratores, às cominações legais, previstas na Lei Estadual 9.433/05, especialmente as definidas no art. 186 do mesmo diploma, garantida a prévia e ampla defesa em processo administrativo, bem como as condutas previstas na legislação específica, especialmente a Lei nº 10.520/02, art. 7º e Decretos Judiciários nº 12/03, 44/03 e 28/08.

18.4. À recusa da assinatura do contrato ou instrumento equivalente e a inexecução contratual, seja parcial ou total, inclusive por atraso injustificado na execução do contrato, serão aplicadas, sem prejuízo da rescisão unilateral do contrato, e de outras cominações legais, a qualquer tempo, MULTA DE MORA de:

18.4.1. 10% (dez por cento) sobre o valor do contrato, em caso de **descumprimento total** da obrigação principal, inclusive no de recusa do adjudicatário em firmar o contrato;

18.4.2. Recusando-se o adjudicatário a subscrever ata de registro de preços, a multa será calculada sobre o valor correspondente ao objeto que lhe foi adjudicado.

18.4.3. Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado o percentual 10% (dez por cento) sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento ou do serviço já realizado.

18.4.4. em caso de atraso no cumprimento da obrigação principal, será aplicado o percentual de **0,3% (três décimos por cento) ao dia,** até o trigésimo dia de atraso, **sobre o valor da parte do fornecimento ou serviço não realizado e de,**

18.4.5. 0,7% (sete décimos por cento) sobre o valor da parte do fornecimento ou serviço não realizado, **por cada dia subsequente ao trigésimo.**

18.5. Na hipótese do item anterior, se a multa moratória atingir o patamar de 10% (dez por cento) do valor global do contrato, deverá salvo justificativa escrita devidamente fundamentada, ser recusado o recebimento do objeto, sem prejuízo da aplicação das sanções previstas neste Edital e em lei.

18.6. As multas previstas neste artigo não têm caráter compensatório e o seu pagamento não eximirá a **CONTRATADA** da responsabilidade por perdas e danos decorrentes das infrações cometidas.

18.7 As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

18.8. Serão punidos com a pena de **SUSPENSÃO TEMPORÁRIA DO DIREITO DE CADASTRAR E LICITAR E IMPEDIMENTO DE CONTRATAR COM A ADMINISTRAÇÃO** aos que incorrerem nos ilícitos previstos nos incisos VI e VII do art. 184 e incisos I, IV, VI e VII do art. 185 da Lei Estadual nº 9.433/05.

18.9. Serão punidos com a pena de **DECLARAÇÃO DE INIDONEIDADE PARA LICITAR E CONTRATAR COM A ADMINISTRAÇÃO,** enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade competente para aplicar a punição, os que incorram nos ilícitos previstos nos incisos I a V do art. 184 e incisos II, III e V do art. 185 da Lei Estadual nº 9.433/05.

18.10. Constitui ilícito administrativo a conduta do licitante que, no pregão eletrônico, em sendo arrematante, não encaminhar, quando convocado, a documentação exigida para o certame, no prazo e na forma estabelecidos no edital, sujeitando-se o infrator, com fundamento no art. 7º da Lei Federal nº 10.520/02, às cominações legais.

18.11. A multa a que se refere este item não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas nesta Lei.

18.12. A multa, aplicada após regular processo administrativo, será descontada dos pagamentos eventualmente devidos pela Administração ou retido da garantia do contratado faltoso quando esta se der por caução em dinheiro.

18.13. Se o valor da multa exceder ao da garantia prestada, além da perda desta, o contratado responderá pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou, ainda, se for o caso, cobrada judicialmente.

18.14. O somatório das multas previstas nos itens acima não poderá ultrapassar o percentual de 10% sobre o valor total do contrato.

18.15. Outras sanções poderão eventualmente ser impostas à CONTRATADA de acordo com a legislação aplicável.

18.16. Toda sanção aplicada será processada pela Comissão Permanente de Cadastro de Fornecedores e Aplicação de Sanções Administrativas do Tribunal de Justiça da Bahia.

19. ACOMPANHAMENTO DOS PRAZOS DE GARANTIA E NÍVEIS MÍNICOS DE SERVIÇO (NMS)

19.1. Quanto à garantia e suporte a serem prestados pela CONTRATADA:

19.1.1. Considerando que a presente demanda se refere à contratação de Serviços com níveis predefinidos pelo fabricante, o Nível Mínimo de Serviço exigido para essa categoria de serviços será baseado no compromisso de qualidade e de prazos definidos no modelo "*Trend Micro™ Premium Support",* definida na Política de Suporte do fabricante da solução.

19.2. Para o atendimento Níveis Mínimos de Serviço, a Contratada deverá atender ao quanto disposto no item 3.5. do Anexo I – Termo de Referência deste Edital.

20. RESCISÃO DO CONTRATO

20.1. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento.

20.2. O **CONTRATANTE** ao longo da vigência do contrato poderá rescindi-lo conforme disposto no art. 168, da Lei nº 9.433/05, motivadamente, desde que seja a **CONTRATADA** notificada, por escrito, com antecedência de 30 (trinta) dias corridos, assegurados o contraditório e a ampla defesa.

20.3. Quando a rescisão ocorrer com base nos incisos I e XVI a XX do art. 167, da Lei nº 9.433/05, sem que haja culpa da **CONTRATADA**, será esta ressarcida dos prejuízos regularmente comprovados que houver sofrido, tendo ainda direito a:

a) devolução da garantia, caso tenha sido exigida;
b) pagamentos devidos pela execução do contrato até a data da rescisão;
c) pagamento do custo da desmobilização.

20.4. No caso de rescisão determinada por ato unilateral da **CONTRATADA** ficam asseguradas à **CONTRATANTE**, sem prejuízo das sanções cabíveis:

a) execução dos valores das multas e indenizações devidas à **CONTRATANTE**;
b) retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à **CONTRATANTE.**

20.5. O contrato poderá ser rescindido por acordo entre as partes, desde que haja conveniência para o **CONTRATANTE** conforme o disposto no inciso II, art. 168, Lei 9.433/2005.

21. REVOGAÇÃO – ANULAÇÃO

21.1. A Administração se reserva ao direito de, com base no art. 122 da Lei Estadual nº 9.433/05, revogar esta licitação, por razões de interesse público decorrente de fato superveniente, devidamente comprovado, pertinente e suficiente para justificar a decisão. Deverá, por outro lado, anulá-la se constatada insanável ilegalidade, baseado em parecer escrito e devidamente fundamentado.

21.2. Não caberá qualquer indenização aos proponentes em caso de revogação ou anulação da presente licitação, ressalvadas as hipóteses legais, cabendo o ônus da prova exclusivamente ao licitante/contratado.

22. DISPOSIÇÕES FINAIS

22.1. A qualquer tempo, antes da data fixada para apresentação das propostas, poderá o Pregoeiro, se necessário, modificar este Edital, hipótese em que deverá proceder à divulgação, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

22.1.1 As modificações do edital serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes. [NOTA: art. 15 do Decreto no 19.896/20]

22.2. O pregoeiro poderá em qualquer fase da licitação, suspender os trabalhos, procedendo ao registro da suspensão e a convocação para a continuidade dos mesmos, bem como promover diligências destinadas a esclarecer ou a complementar a instrução do processo licitatório, desde que não implique em inclusão de documento ou informação que deveria constar originariamente da proposta.

22.3. O pregoeiro poderá, no julgamento da habilitação e das propostas, sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação e classificação. [NOTA: art. 31, caput, do Decreto no 19.898/20]

22.4. Havendo necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata este item, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo,

24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata. [NOTA: art. 31, §1o, do Decreto no 19.898/20]

22.5. Quando todas as propostas forem desclassificadas ou todos os licitantes forem inabilitados, o pregoeiro poderá, caso se esta funcionalidade estiver disponível no sistema, suspender o pregão e estabelecer uma nova data, com prazo não superior a 03 (três) dias úteis, para o recebimento de nova proposta ou nova documentação, após sanadas as causas que motivaram a desclassificação ou inabilitação. [NOTA: art. 31, §2o, do Decreto no 19.898/20]

22.6. O pregoeiro poderá, a qualquer tempo, negociar com o proponente da melhor oferta aceitável, visando obter preço menor.

22.7. Os participantes da licitação têm direito público subjetivo à fiel observância do procedimento estabelecido neste Decreto e qualquer interessado poderá acompanhar o seu desenvolvimento. [NOTA: art. 39, §2o, do Decreto no 19.898/20]

22.8. A instrução do processo licitatório poderá ser realizada por meio de sistema eletrônico, cujos documentos, constantes dos arquivos e registros digitais, serão válidos para todos os efeitos legais. [NOTA: art. 39, §1o, do Decreto no 19.898/20]

22.8.1 Os atos do procedimento do pregão eletrônico serão disponibilizados para acesso livre, nos termos da legislação pertinente, ressalvados os documentos sigilosos, apenas enquanto perdurar esta condição. [NOTA: art. 39, §3o, do Decreto no 19.898/20]

22.8.2 Os arquivos e os registros digitais relativos ao pregão eletrônico serão documentados no processo respectivo com vistas à aferição de sua regularidade pelos agentes de controle, nos termos da legislação pertinente. [NOTA: art. 39, §4o, do Decreto no 19.898/20]

22.9. A CONTRATADA respondera integralmente pela qualidade do fornecimento e dos serviços pós-venda, incluindo-se nessa responsabilidade a qualificação técnica dos profissionais intervenientes.

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

22.11. Os casos omissos serão dirimidos pelo Pregoeiro, com observância da legislação em vigor, considerando as disposições legais contidas no preâmbulo deste edital.

22.12. As despesas decorrentes da execução de cada contratação correrão à conta da dotação orçamentária correspondente a cada órgão ou entidade solicitante.

22.13. Para quaisquer questões judiciais oriundas do presente Edital, fica eleito o Foro da Comarca de Salvador, Estado da Bahia, com exclusão de qualquer outro, por mais privilegiado que seja.

22.14. São partes indissociáveis deste Edital os anexos relacionados deste Instrumento Convocatório

Salvador, 06 de março de 2023.

Fernanda Ferreira Ribeiro
Pregoeira

Antonio Henrique Sampaio Garcia
Chefe do NCL

ANEXO I – TERMO DE REFERÊNCIA

1 OBJETO

Constitui objeto do presente Termo de Referência a contratação de solução de segurança da informação, composta de software de segurança para usuário final e cargas de trabalho híbridas, proteção contra ameaças avançadas incluindo fornecimento de appliance, proteção contra ameaças de nuvem e gerenciamento de conformidade, com detecção e resposta e gerenciamento proativo e corretivo das soluções, para o Tribunal de Justiça do Estado da Bahia, conforme exigências estabelecidas neste documento e seus anexos.

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 MOTIVAÇÃO

De acordo com o Relatório de Riscos Globais 2022 do Fórum Econômico Mundial, a crescente dependência dos sistemas digitais está mudando fundamentalmente a sociedade, e as ameaças à segurança cibernética estão ultrapassando a capacidade de prevenção e respostas da sociedade.

Os ataques às infraestruturas críticas, a desinformação e as fraudes estão afetando a confiança do público nesses sistemas. À medida que o crime cibernético avança, as organizações precisam atualizar a estratégia e a arquitetura de segurança cibernética para continuar atendendo as demandas da sociedade, preservando o exercício da cidadania e das liberdades individuais, mesmo em situações adversas de eventuais ataques cibernéticos. Além disso, a LGPD, Lei Geral de Proteção de Dados, determina a adoção de medidas técnicas e administrativas eficazes para a proteção dos dados pessoais.

Atualmente, o Tribunal de Justiça do Estado da Bahia, possui em seu parque tecnológico aproximadamente 13.000 estações de trabalho, 900 servidores virtuais, 13.400 usuários ativos de rede além de storages e outros hosts sensíveis. Cada um desses ativos guarda informações que precisam estar protegidas de ações ilegítimas.

Para prover tal proteção, atualmente o TJBA faz uso das diversas ferramentas de segurança da informação desenvolvidas pela Trend Micro. A solução contratada envolve os seguintes produtos: Trend Micro Smart Protection Suite, Deep Security e Trend Micro Analyser. A suite Smart Protection é composta pelos módulos OfficeScan, Intrusion Defense Firewall, Scanmail e Advanced, e-mail and mail gateway e é voltada prioritariamente para proteção de estações de trabalho (endpoints). Já a solução Deep Security, voltada para servidores, é composta pelas soluções de Network Security e Malware Prevention. A proteção atual inclui ainda funcionalidades de virtual patching e HIPS (Host Intrusion Prevention System), proteção de acesso WEB (Web Reputation), proteção anti-spam para o serviço de correio eletrônico e funcionalidade de SandBox, todas compartilhadas entre as estações de trabalho e servidores.

Cada um dos módulos da solução atualmente instalada e em operação cobre uma determinada camada de segurança, funcionando como sensores individuais de modo que, quando integrados, ampliam a superfície de proteção do ambiente do TJBA.

As soluções desenvolvidas pela Trend Micro encontram-se em uso neste órgão desde 2005, ano no qual as primeiras licenças foram adquiridas através do Pregão Eletrônico 048/2005. Nesse primeiro momento foram contratadas 3700 licenças. Em 2009, mais 2300 licenças adicionais foram adquiridas pelo Pregão Eletrônico n° 091/2009, e através de contratações conseguintes o quantitativo foi crescendo gradativamente, até atingir o patamar médio de 1400 licenças. Nesse período também foram adquiridas licenças da ferramenta DDI (Deep Discovery Inspection), através do contrato 36/17-AQ desenvolvida pelo mesmo fabricante. À época, a ferramenta trouxe vários benefícios para a proteção do ambiente do Tribunal, porém, por motivos diversos suas licenças não puderam ser renovadas.

Além das aquisições das licenças perpétuas, ano após ano são necessárias contratações de suporte para tais licenças, o que permite a atualização das aplicações com as correções lançadas pelo fabricante, além de se ter disponível o suporte especializado para casos de necessidade. A última renovação desse suporte foi realizada pelo contrato 14/20-S, que vigorou por 12(doze) meses e teve sua primeira aditivação feita pelo AS 31/21. Esse último findou em 31/03/2022 e sua renovação se deu através do processo TJ-ADM-2022/05327, aditivo 29/22-AS.

De acordo com nota pública disponibilizada pelo fabricante[1] , a suíte de softwares atualmente utilizada pelo TJBA está no fim de sua vida, tecnicamente falando, entrando em EOL (End of Life)[2] , sendo descontinuada em março de 2023 e assim, a impossibilidade de proceder com novo aditamento temporal do contrato existente. Com isso a necessidade urgente de contratação de uma nova solução, para dar continuidade aos serviços de segurança e proteção que já são utilizados no TJBA, e evitando ao máximo, a exposição do Tribunal a ameaças e riscos cibernéticos e, consequentemente, evitando prejuízos na prestação jurisdicional. Uma eventual descontinuidade na contratação dessas ferramentas colocaria o Poder Judiciário da Bahia em grave risco cibernético, uma vez que não seria possível manter as assinaturas de segurança

[1] https://success.trendmicro.com/dcx/s/solution/000285899?language=en_US&sfdcIFrameOrigin=null
[2] Termo que se refere aos produtos fornecidos aos clientes, que indica que o produto está no fim da sua vida útil ou sendo descontinuado.

atualizadas.

Diante da impossibilidade de renovação do pacote de suporte da suíte contratada e com a evolução por parte das ameaças e ferramentas, entende-se que, apesar do último contrato contemplar serviços especializados de suporte dos componentes dos softwares de Anti-malware, anti-Spam e Sandbox, é necessário que este Tribunal busque não somente a renovação de uma suíte de segurança equivalente à já contratada, mas também uma arquitetura atualizada que traga ferramentas avançadas que cubram todo o perímetro de segurança da informação.

A atualização da arquitetura de segurança cibernética é um requisito obrigatório para se fazer frente aos desafios atuais. Para tanto é imprescindível que se adote uma plataforma abrangente e integrada, capaz de visualizar, analisar, correlacionar e responder a eventos suspeitos na rede, nos e-mails, nas ferramentas de colaboração, nos notebooks e estações de trabalho, nos servidores locais, nas cargas de trabalho em nuvem, e na camada de aplicação. É imprescindível ainda, que a solução se conecte a um ecossistema de cibersegurança global com inteligência artificial que atue contra ameaças conhecidas pela comunidade internacional. Também é necessário que haja integração com ferramentas de terceiros, para que sejam aproveitadas, na composição da arquitetura de segurança, ferramentas já contratadas pelo TJBA, além de apresentar painel com os riscos, detecções, ameaças, vulnerabilidades e ataques aos quais o TJBA esteja relacionado.

Com relação às novas demandas surgidas a partir das adoções feitas aos serviços de nuvem, é requerida uma nova estratégia de cibersegurança capaz de identificar, proteger detectar, responder e recuperar o ambiente de ataques cibernéticos com características diferentes do que ocorria até então, quando as aplicações eram todas hospedadas em data centers tradicionais. O uso de estruturas mais ágeis, como SaaS (Software As a Service), PaaS (Platform As a Service), IaaS (Infrastructure As a Service), containers e serverless, exigem uma tecnologia de cibersegurança capaz de lidar com os requisitos desses novos ambientes.

2.2 OBJETIVOS

A contratação da solução de segurança tem por objetivos:

a) Manter o software da solução ora implantada, visando proteção de rede, detecção e prevenção contra ameaças;
b) Minimizar os riscos de interrupção da proteção de cibersegurança;
c) Proteger os ambientes on premises e em nuvem, de maneira integrada;
d) Ampliar as camadas de proteção contra riscos cibernéticos com ferramentas avançadas.

2.3 BENEFÍCIOS

Os benefícios esperados com esta contratação são:

a) Garantir a alta disponibilidade e integridade do ambiente tecnológico deste Tribunal;
b) Aumentar a segurança da rede, com agentes instalados em cada computador, minimizando os problemas relacionados às estações de trabalho, cite-se: Disseminação de pragas virtuais (vírus, trojans, malware e códigos maliciosos);
c) Promover melhorias no processo de monitoramento, através da predefinição e personalização de gráficos de monitoramento e envio de notificações;
d) Garantir o aproveitamento do conhecimento histórico acerca das ferramentas;
e) Garantir suporte técnico avançado 24X7;
f) Promover a evolução das ferramentas para modelo SaaS em nuvem.

2.4 ALINHAMENTO ESTRATÉGICO

A demanda está alinhada com os objetivos estratégicos da Resolução 396/2021 do CNJ.
A demanda, embora não contemplada no Plano de Contratação 2022, devido a urgente necessidade de proteção dos ambientes on premisses e em nuvem, e buscando o preenchimento dos requisitos, constantes no art. 12, §4º, §5º e §6º da Resolução nº 182/13 do CNJ, obteve autorização da Presidência do Poder Judiciário da Bahia, para que fosse contratada.

2.5 REFERÊNCIA AOS ESTUDOS PRELIMINARES

Este Termo de Referência foi elaborado com base nas informações contidas no Documento de Oficialização da Demanda (DOD) encaminhado pela Coordenação de Produção e Suporte Técnico – COTEC, para a Secretaria de Tecnologia da Informação e Modernização – SETIM e no conteúdo do Estudo Preliminar, desenvolvido pela equipe de planejamento da contratação.

Todos os documentos encontram-se no Processo Administrativo TJ-ADM-2022/19737 de que trata esta contratação, em tramitação no SIGA.

2.6 RELAÇÃO ENTRE A DEMANDA PREVISTA E A CONTRATADA

Conforme descrito, o TJBA faz uso das ferramentas Trend Micro desde o ano de 2005. Desde então as soluções se mostram confiáveis, vez que não se tem registros de incidentes graves de segurança nesse ínterim. Além disso, dado todo esse período de uso das ferramentas, é fato de que os conhecimentos acerca da plataforma Trend Micro estão disseminados dentro do órgão e são demasiado importantes para sua segurança.

Porém, o modelo de licenças atual é pouco ou nada flexível quanto ao ambiente onde as licenças serão instaladas, e considerando o contrato de nuvem pública vigente (45/21-S), é importante que se tenha disponíveis licenças que possam ser instaladas também em um ambiente diferente do on premises. Isso para que se mantenham seguros os ativos dispostos fora do data center do TJBA. Corroborando com o citado, tem-se o fato da recente contratação de licenças da plataforma de colaboração Microsoft 365, dada através do contrato 23/21-S, dispondo de uma gama de ferramentas colaborativas para as quais também se fará necessário incluir a proteção. A respeito disso, o TJBA está nas últimas etapas de migração das caixas de e-mail para a nuvem, porém a licença da ferramenta de anti-spam contratada não permite integração a esse novo ambiente.

Acrescente-se ainda a constante aquisição de desktops para atualização do parque computacional. Somente no ano de 2022, foram adquiridos ao menos 2.000 equipamentos deste tipo e, portanto, mais 2.000 equipamentos que precisarão estar protegidos.

Assim, entende-se que as demandas previstas e projetadas pela Coordenação de Produção e Suporte Técnico – COTEC a serem atendidas pela contratação da solução de segurança de perímetro, serão cobertas em sua plenitude, visando ampliação e modificação de plataforma das Ferramentas Trend Micro durante o período de vigência contratual, através do contrato estabelecido entre o CONTRATANTE e a CONTRATADA.

Abaixo estão listados os itens da composição da solução:

ITEM	DESCRIÇÃO DO ITEM	QTD.
1	Software de segurança para usuário final, contendo ambiente isolado e seguro para teste de novas ameaças, com visibilidade, detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	14200 Usuários
2	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	1001 Servidores Virtuais
3	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses.	1 Appliance
4	Solução de proteção para serviços em nuvem com validação de melhores práticas, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	10 Cloud Accounts
5	Solução de proteção para áreas de armazenamento de arquivos em nuvem, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	10 Buckets de Nuvem
6	Treinamento oficial do fabricante	6 Treinamentos
7	Gerenciamento especializado, proativo, preventivo e corretivo de ameaças por 24 (vinte e quatro) meses	24 Meses

Tabela 01

Conforme já citado anteriormente, o TJBA, possui em seu parque tecnológico aproximadamente 13.000 estações de trabalho, 900 servidores virtuais, 13.400 usuários ativos de rede além de storages e outros hosts sensíveis.

Portanto, observa-se que os números elencados na tabela acima são compatíveis com a demanda atual e uma eventual expansão, além de serem corretamente equivalentes com os números de licenciamento e quantitativos dos contratos já citados que a presente solução irá proteger.

2.7 ANÁLISE DE MERCADO DE TIC

Sendo uma solução comum de mercado, existem diversos fabricantes que podem oferecer soluções de segurança de perímetro, com diferentes graus de qualidade e diversos preços a serem pagos, mas dada complexidade do ambiente e a quantidade de ativos existentes, uma migração para outra ferramenta com um ecossistema diferente do que já está atualmente implantando no TJBA, traria inúmeros outros riscos para os serviços disponibilizados, já que seria necessário

um período razoável para que todo o parque estivesse coberto e operacional, tempo no qual o TJBA estaria exposto à diversos riscos cibernéticos. Esse é um ponto sensível que gera bastante temor e deve ser considerado, haja vista incidentes recentes envolvendo órgãos de justiça por todo país, paralisando suas atividades e com consequências diretas para os jurisdicionados.

2.7.1 SOLUÇÕES CONTRATADAS POR ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA

Foram encontradas contratações recentes, que traziam como componente, a contratação da solução de segurança com a ferramenta Trend Micro, objeto desta contratação, quais sejam:

TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS – TEC/GO
Pregão Eletrônico nº 009/20
Objeto: Contratação de empresa especializada para renovação de solução de segurança para e-mails (antispam), serviços de garantia com atualização continuada (upgrade/update) e serviço de suporte técnico 5X8 por 12 meses, na ferramenta Trend Micro utilizada por este Tribunal, relacionado com a necessidade de prover segurança para o ambiente.

TRIBUNAL DE JUSTIÇA DO ESTADO DE PARÁ – TJPA
PROCESSO ADMINISTRATIVO PA-PRO-2021/01602
Objeto: Contratação de empresa para fornecimento de subscrição de softwares de segurança, incluindo garantia, atualização de versão, suporte técnico por 24 meses, transferência de conhecimento e serviços técnicos especializados, conforme especificações e quantidades previstas no termo de referência, para atender as necessidades do Tribunal de Justiça do Estado do Pará.

SECRETARIA DE ESTADO DA ADMINISTRAÇÃO E PREVIDÊNCIA DO PIAUÍ – SEADPREV/PI
Pregão Eletrônico nº 009/2021
Objeto: Contratação de Solução unificada de segurança para proteção de e-mail, proteção de Endpoint e proteção contra-ataques, com garantia de 36 meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades dos órgãos e entes da Administração Pública, de acordo com as especificações técnicas contidas no Termo de Referência.

Embora a contratação da solução em pauta seja comum entre os órgãos públicos analisados, existe uma significativa variedade na composição de cada objeto de contratação que, destinados às mais variadas peculiaridades, visam atender às necessidades de cada contratante. Portanto, não é uma tarefa evidente encontrar contratações de solução com características semelhantes às definidas para o TJBA.

Dentre as contratações encontradas, foram observadas diferenças entre o tempo de vigência, número de licenças e precificação em relação ao TJBA, permitindo apenas uma comparação limitada, mas, ainda assim, evidenciando o caráter comum desse tipo de contratação.

2.7.2 DEFINIÇÃO E JUSTIFICATIVA DA SOLUÇÃO ADOTADA

Na essência da demanda encontra-se a necessidade de manter em atividade a solução já implantada, evitando o risco de descontinuidade das operações de segurança. As soluções desenvolvidas pela Trend Micro encontram-se em uso no Poder Judiciário do Estado da Bahia, desde 2005, e desde então é um recurso indispensável para a segurança da rede corporativa do Poder Judiciário. A implantação de uma nova solução de segurança num ambiente tecnológico complexo e distribuído como o que se tem no TJBA não é trivial. Além da perda do investimento em licenças iniciais – relativamente irrelevante, no caso das soluções antivírus, posto que o custo mais significativo é dado pelo serviço de atualização permanente – a implantação de uma nova solução envolveria esforços de dimensionamento, projeto, instalação, configuração, customização, treinamento dos analistas, distribuição de componentes para equipamentos servidores e estações de trabalho em múltiplas comarcas do Estado etc. Diante desses fatos e dos riscos apresentados, a estratégia encontrada pela equipe de contratação que demonstra maior segurança e melhor custo-benefício, dar-se por manter o ecossistema ora instalado, atualizando as ferramentas e a arquitetura de segurança do ambiente já implantados

Embora existam diversas soluções possíveis para atender a demanda, razões de peso aconselham manter a solução já utilizada. Além das já mencionadas nos itens anteriores, listam-se:

- Continuidade operacional: Trata-se de uma solução complexa, já implantada e disseminada por toda a estrutura de TIC do TJBA, homologada, compatibilizada e com servidores treinados para administrá-la e dar-lhe manutenção. Nesse tocante, há de se considerar que, justamente pela complexidade do parque computacional, o órgão levou vários anos para alcançar a cobertura completa do ambiente, de forma que é prudente e razoável se optar pela preservação de investimento de tempo e esforço já dedicados.
- Eficiência: Por mais de uma década, perpassando diversas gestões administrativas, a solução implantada foi utilizada, atualizada e expandida com resultados satisfatórios. Ademais, o modelo de solução ora proposto também leva em conta as mais recentes tecnologias de mercado, especialmente por se tratar de uma solução já no modelo Cloud Native, ou seja, em nuvem, onde o fabricante é responsável pela plataforma e sua operacionalização, enquanto o TJBA como cliente irá consumir os benefícios da solução, diminuindo seu custo operacional de manter a gerência das soluções em ambiente local.

• Integração: Praticamente todas as funções que caracterizam os componentes da solução podem ser encontradas em outros produtos de mercado. Porém, trata-se de abordagens parciais, pois estão disponíveis em fabricantes diferentes e, portanto, são soluções isoladas. Para compor uma solução de conjunto equivalente à contemplada no contrato, seria preciso integrar produtos de diversos fabricantes, com previsíveis dificuldades de compatibilidade, gerenciamento e segurança. No caso da solução em tela, em que se trata de um único fabricante, obtém-se a vantagem de poder implementar um ecossistema de segurança, em que todas as soluções se integram nativamente e sem limitação de funcionalidades, vantagem que não é percebida quando se integram produtos de diferentes fabricantes.
• Qualidade: A posição de liderança da Trend é atestada por diversos órgãos de consultoria independente. Embora, nos dois últimos relatórios, tenha perdido a posição de proeminência que manteve durante 14 anos consecutivos, ainda integra o grupo das empresas líderes no quadrante mágico Gartner relativo a produtos voltados à proteção de endpoints.
• Economicidade: Sob o ponto de vista econômico, a manutenção da atual solução também se revela vantajosa, já que a sua substituição traria consigo todo o ônus relacionado à nova instalação, configuração e treinamento. Do ponto de vista administrativo, percebe-se uma economicidade da gestão e fiscalização contratual, vez que, toda a solução estaria contemplada por um único contrato administrativo.

Além das vantagens econômica, técnica e estratégica citadas para a continuidade do serviço, destaca-se ainda que a solução existente atende as necessidades do TJBA, necessitando apenas, como já informado, de atualizações e evoluções.

Desta forma, a equipe de planejamento da contratação entende que a vantagem está claramente demonstrada, pois optou pela continuidade, ou seja, a padronização em suas unidades, porque já utiliza o produto, tendo ainda demonstrado vantagens técnicas, já em uso em seus ambientes e nuvem. Acrescente-se ainda o aproveitamento do conhecimento, da total compatibilidade dos ambientes, da facilidade de integração e operação, não demandando qualquer arranjo tecnológico para o pleno funcionamento da solução, eliminando assim o risco a operação do ambiente tecnológico do Tribunal.

Ratifica-se, portanto, que a contratação de uma outra solução seria mais onerosa para o TJBA, tanto em aspectos financeiros quanto para o conhecimento.

2.8 NATUREZA DO OBJETO

O objeto consiste na contratação de serviços de licenciamento com direito de uso, suporte técnico, suporte especializado e garantia, incluindo também a contratação de hardware como item de menor peso.

Portanto, a predominância da demanda encontra-se na contratação de serviços, com características comuns e usuais disponíveis no mercado de TIC, cujos padrões de desempenho e de qualidade são objetivamente definidos na especificação do fabricante, enquadrando-se, portanto, na definição de bem comum, conforme parágrafo único do artigo 1º da lei que institui o pregão eletrônico (Lei 10.520/2002).

Embora exista a necessidade de ser manter o fabricante, o objeto desta contratação pode ser fornecido por diversas revendas e possui características comuns e usais encontradas. Deve-se frisar que a solução de serviços é comercializada por representantes comerciais do fabricante, prestada pelos mesmos parceiros, e não possuirá mão de obra residente.

2.8.1 VIGÊNCIA DO CONTRATO

A contratação da solução de que trata o presente processo terá início na data de assinatura do contrato, com vigência de 24 (vinte e quatro) meses, prorrogáveis nos termos do artigo 140 da Lei Estadual nº 9.433/05 e de acordo com a conveniência das partes.

2.8.2 REAJUSTE CONTRATUAL

Dentro do prazo de vigência, em caso de prorrogação do contrato mediante solicitação da CONTRATANTE, os valores contratados poderão ser reajustados, aplicando o ICTI (Índice de Custos de Tecnologia da Informação). Caso o índice estabelecido para reajuste venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação vigente.

2.9 PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

Apesar de a contratação prever ferramentas diferentes como parte de um todo, estes itens devem ser fornecidos por um único fabricante, pois o licenciamento, suporte e garantia necessitam ser compatíveis entre si e prestados por um mesmo fornecedor, de modo que se evite terceirização de responsabilidades em casos de crises com incidentes de segurança. Assim, o objeto não pode ser composto por ferramentas de fabricantes diferentes, sob vista de impedir o pleno funcionamento da solução. Portanto, por ser necessário que todas as ferramentas componentes da solução estejam integradas de maneira nativa e façam parte do mesmo ecossistema de segurança, não se permite o parcelamento do objeto.

2.10 MODALIDADE, TIPO DE LICITAÇÃO E CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA

Conforme expressado no Item 2.8, o objeto possui características comuns e usuais encontradas no mercado de TIC e, portanto, sugere-se a modalidade Pregão Eletrônico com seleção da melhor proposta pelo menor preço global.

2.10.1 LIMITES MÁXIMOS DE PREÇO

Considerando as propostas apresentadas pelos fornecedores consultados, os limites máximos de preços aceitáveis para cada item durante 24(vinte e quatro) meses da vigência do contrato são dados pela tabela a seguir:

ID	ITEM	QTD.	Valor Unitário	Valor Total
1	Software de segurança para usuário final, contendo ambiente isolado e seguro para teste de novas ameaças, com visibilidade, detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	14.200	R$ 431,49	R$ 6.127.158,00
2	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	1.001	R$ 2.741,93	R$ 2.744.671,93
3	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante 24 (vinte e quatro) meses.	1	R$ 2.765.162,35	R$ 2.765.162,35
4	Solução de proteção para serviços em nuvem com validação de melhores práticas, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	10	R$ 15.137,50	R$ 151.375,00
5	Solução de proteção para áreas de armazenamento de arquivos em nuvem, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	10	R$ 58.429,53	R$ 584.295,30
6	Treinamento oficial do fabricante	6	R$ 12.775,34	R$ 76.652,04
7	Gerenciamento especializado, proativo, preventivo e corretivo de ameaças por 24 (vinte e quatro) meses	24	R$ 70.918,11	R$ 1.702.034,72
			TOTAL	**R$ 14.151.349,34**

Tabela 02

Considerando que a contratação inclui diversos itens e, com o objetivo de evitar desequilíbrio na composição dos preços individuais por item, não serão aceitas propostas cujo valor global esteja dentro do limite máximo, mas não estejam cumprindo o limite máximo do item indicado na tabela.

Como se pode observar na tabela, o limite máximo de valor aceitável, durante 24 (vinte e quatro) meses de vigência do contrato, é dado por:

Valor Global: R$ 14.151.349,34 (Quatorze milhões, cento e cinquenta e um mil, trezentos e quarenta e nove reais e trinta e quatro centavos)

Todas e quaisquer despesas necessárias ao cumprimento do objeto desta contratação, tais como mão de obra, impostos, tributos, encargos e contribuições sociais, fiscais, parafiscais, fretes, seguros, transporte, estadia, alimentação e demais despesas inerentes, correrão por conta da CONTRATADA, não cabendo ao CONTRATANTE, o reembolso de despesas com transporte, hospedagem e outros custos operacionais, não previstos neste Termo de Referência, que devem ser de exclusiva responsabilidade da CONTRATADA.

2.10.2 HABILITAÇÃO E QUALIFICAÇÃO TÉCNICA

Para fins de habilitação técnica, a licitante arrematante deverá apresentar, na forma e nos prazos indicados no edital.

a) Documento de comprovação informando que a licitante é revendedora ou distribuidora autorizada do fabricante;
b) Atestado (s) de capacidade técnica em nome da empresa, emitido (s) por pessoa (s) jurídica (s) de direito público ou privado, que, individualmente ou somados, comprove (m) o desempenho satisfatório na execução dos serviços abaixo listados:

i. Fornecimento de, no mínimo, 3.500 licenças de software de segurança TrendMicro para Endpoint, compatível com o item 1 da solução, constante na tabela 02;

ii. Fornecimento de, no mínimo, 250 licenças de solução de segurança para servidores, compatível com o item 2 da tabela 02;

iii. Fornecimento e Instalação de, no mínimo, 1 Appliance de segurança do Tipo Inspeção de rede com o mínimo de 1 Gbps de Throughput;

iv. Prestação de serviço gerenciado de suporte especializado nas soluções TrendMicro por, no mínimo, 12 meses;

Todas as informações citadas acima deverão constar de forma explícita no(s) atestado(s).

Admite-se mais de um atestado com vistas a comprovar o atendimento a todos os requisitos de capacidade técnica que asseguram a similaridade do objeto.

No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da licitante. Serão consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa licitante, e ainda as que tenham pelo menos uma pessoa física ou jurídica como sócia em comum.

Somente serão aceitos atestados referentes a contratos já encerrados ou referentes a contratos cuja execução já tenha alcançado pelo menos 50% do volume de seu respectivo objeto, no que concerne aos serviços que se pretende atestar.

É preferível que os atestados emitidos por pessoa jurídica de direito privado contenham assinatura digital certificada ou com reconhecimento de firma, que assegure sua autenticidade. Caso a assinatura do responsável técnico não contenha elemento de autenticação, a Contratante se resguarda ao direito de realizar diligência para solicitar documentos a fim de sanar eventuais dúvidas quanto ao referido atestado.

Tais declarações deverão ser emitidas em papel timbrado, com assinatura, identificação e telefone do emitente.

A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s).

O Tribunal de Justiça do Estado da Bahia se reserva ao direito de realizar diligências para averiguar a veracidade dos documentos e declarações junto à pessoa jurídica emissora dos Atestados e/ou Declarações, visando obter informação sobre o serviço prestado e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

Quando solicitado através de diligência, o licitante deverá prontamente disponibilizar todas as informações necessárias à comprovação da legitimidade dos respectivos atestados, apresentando, dentre outros documentos, a cópia do contrato que deu suporte à contratação, o endereço atual da contratante e o local em que foram prestados os serviços, sob pena de inabilitação.

Os referidos documentos devem ser apresentados em língua portuguesa, com a ressalva de que todos os que forem emitidos em língua estrangeira deverão ser acompanhados da correspondente versão em português, assinada por tradutor juramentado.

2.10.3 DA SUBCONTRATAÇÃO[3]

Não será admitida a Subcontratação.

2.10.4 DO CONSÓRCIO[4]

Não será admitido o Consórcio.

2.10.5 ALTERAÇÃO CONTRATUAL SUBJETIVA[5]

Será admitida, caso necessário, a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que:

[3] Art. 160 da Lei Estadual 9.433/05
[4] Art. 105 da Lei Estadual 9.433/05
[5] Art. 78 – inciso XI da Lei 8.666/93

sejam observados, pela nova pessoa jurídica, todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado; e haja a anuência expressa da Administração à continuidade do contrato.

2.11 IMPACTO AMBIENTAL DA CONTRATAÇÃO

Não foram encontrados riscos ambientais significativos, em decorrência do fornecimento dos itens que compõem a contratação de segurança de servidores e proteção de endpoints.

2.12 CONFORMIDADE TÉCNICA E LEGAL

Os serviços, que constituem o objeto desta contratação, deverão estar em conformidade com as seguintes normas técnicas e legais:

a) Lei Federal 13.709/2018 – Lei Geral de Proteção de Dados, a qual dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
b) Política de Segurança da Informação e suas normas, Decreto Judiciário nº 474[6] , de 16/08/2019.

2.13 OBRIGAÇÕES DA CONTRATADA

a) Fornecer o objeto adjudicado em estrita conformidade com as especificações, quantidades, prazos e demais condições estabelecidas no Edital e seus anexos;
b) Participar de reunião de alinhamento a ser realizada em data e horário a ser definido pelo CONTRATANTE, nos termos estabelecidos no Item 3.3.1 – Reunião de Alinhamento;
c) Designar e apresentar o preposto do contrato no ato da reunião de alinhamento;
d) Estar disponível para realizar reuniões periódicas com o CONTRATANTE, podendo este último, em atenção às circunstâncias específicas, dispensar reuniões programadas ou convocar, em caso de necessidade, reuniões extraordinárias, às que um representante da CONTRATADA deve comparecer no prazo máximo de dois dias úteis;
e) A CONTRATADA deverá responsabilizar-se solidariamente pela execução completa e satisfatória do fornecimento e dos serviços associados, por meio do gerenciamento dos seus recursos humanos e técnicos, assim como, não poderá se eximir dessa obrigação, ainda que parcialmente, atribuindo quaisquer falhas ou deficiências à imperícia de pessoal ou a erros de especificações;
f) Quando do comparecimento às dependências da CONTRATANTE, promover, por sua conta e risco, o transporte de seus empregados, materiais e utensílios necessários envolvidos nas atividades motivo desta contratação, até às instalações do CONTRATANTE;
g) Quando do comparecimento às dependências da CONTRATANTE, o preposto e os colaboradores da CONTRATADA deverão estar devidamente identificados com crachá no qual conste seu nome, o nome da empresa e a função desempenhada;
h) Respeitar e fazer com que seus empregados respeitem as normas de segurança, disciplina e demais regulamentos vigentes no Poder Judiciário da Bahia, bem como atentar para as regras de cortesia no local onde serão executados os serviços objeto do contrato;
i) Facilitar por todos os meios a seu alcance a ampla ação fiscalizadora do CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem dirigidas;
j) Utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas no contrato, edital e seus anexos;
k) Pagar os salários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços contratados, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vale-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhes defeso invocar a existência deste contrato para eximir-se destas obrigações ou transferi-las para o CONTRATANTE;
l) Manter o sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do Contrato, respeitando todos os critérios estabelecidos no termo de confidencialidade anexo ao certame;
m) Promover, caso necessário, intermediação junto ao fabricante, para garantir o suporte remoto, fornecimento de manuais e acompanhamento necessário para transferência tecnológica e todas as demais opções de interação com a CONTRATANTE, em sua língua nativa – Português do Brasil;

2.14 OBRIGAÇÕES DO CONTRATANTE

Em conformidade com as obrigações resultantes da Lei nº 9433/05, o TJBA deverá:

a) Designar servidores para acompanhamento e fiscalização do contrato, conforme disposto no art. 16 da Resolução

[6] www7.tj.ba.gov.br/secao/lerPublicacao.wsp?tmp.mostrarDiv=sim&tmp.id=22913&tmp.secao=9

nº 182/2013 do Conselho Nacional de Justiça – CNJ e Norma Geral de Contratações do TJBA.
b) Exercer a fiscalização dos serviços, podendo recusar qualquer serviço que não esteja de acordo com as condições estabelecidas neste termo.
c) Assegurar-se da boa prestação dos serviços, verificando sempre seu bom desempenho.
d) Atestar, por intermédio de servidor especialmente designado, as notas fiscais referentes aos serviços e fornecimentos prestados de forma satisfatória.
e) Efetuar o pagamento devido à CONTRATADA, dentro do prazo estipulado, desde que cumpridas todas as formalidades e exigências contratuais.
f) Zelar para que, durante a vigência do contrato, sejam cumpridas as obrigações assumidas por parte da CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.
g) Manter em arquivo, junto ao processo administrativo ao qual está vinculado o presente termo, toda a documentação a ele referente.
h) Disponibilizar todas as informações necessárias para o desenvolvimento dos trabalhos.
i) Fornecer a infraestrutura necessária para o pleno funcionamento dos Serviços, seguindo as especificações técnicas fornecidas pela CONTRATADA e dentro das normas ABNT relacionadas. Entende-se como infraestrutura os recursos computacionais necessários para a execução da plataforma.
j) Validar e aprovar os serviços executados, em conformidade com as regras e requisitos estabelecidos no ANS (Acordo de Níveis de Serviço) refletindo a qualidade entregue em conformidade com o IMR (Instrumento de Medição de Resultado)
k) Providenciar o acesso controlado dos profissionais da CONTRATADA ao ambiente de TI, incluindo bibliotecas de programas, políticas, normas, procedimentos, metodologias, bases de dados, ferramentas, de acordo com pré-requisitos definidos nas comunicações formais de demanda.
l) Aplicar as sanções conforme previsto no contrato.
m) Gerir e fiscalizar, quantitativa e qualitativamente, a execução das demandas por meio do acompanhamento das atividades desenvolvidas e resultados obtidos, observando os prazos e produtos acordados com vistas a efetuar eventuais ajustes e correções de rumo.

3 DETALHAMENTO DO OBJETO

3.1 MODELO DE EXECUÇÃO E DE GESTÃO DO CONTRATO

A execução do Contrato seguirá uma metodologia de trabalho baseada no conceito de Delegação de Responsabilidades. Ao CONTRATANTE caberá a definição das demandas e a gestão qualitativa dos resultados a serem obtidos por meio das atividades desenvolvidas dentro dos prazos e produtos acordados.

À CONTRATADA caberá a responsabilidade pela execução operacional dos serviços, por meio do gerenciamento dos seus recursos humanos e técnicos.

Todo e qualquer serviço somente poderá ser iniciado pela CONTRATADA após aprovação formal pelo CONTRATANTE, devendo obedecer rigorosamente aos requisitos descritos neste Termo de Referência.

3.1.1 SERVIÇOS A SEREM EXECUTADOS PELA CONTRATADA

3.1.1.1 Serviços especializados de suporte avançado da CONTRATADA e/ou Fabricante por 24 meses

a) A CONTRATADA deverá fornecer os pacotes de serviços de garantia, atualização e suporte para os produtos que compõem a solução, de acordo com as definições constantes no Item 3.5.
b) Fornecer e instalar, sempre que forem disponibilizadas, versões ou atualizações de Software da Solução sem custo adicional.
c) Permitir que a CONTRATANTE se comunique diretamente com o fabricante no regime 24 horas por dia, 7 dias por semana para abertura de casos de suporte relativos ao funcionamento das soluções no escopo, bem como a ameaças no ambiente ou dúvidas gerais sobre segurança da informação.
d) O fabricante deverá fornecer acesso a um gestor de serviços para comunicações gerais acerca do ambiente e das entregas contratadas, agindo como um ponto único de contato.
e) O gestor de serviço deverá entregar relatórios sobre o desempenho e entregas de forma periódica durante o contrato.
f) Quando necessário, a CONTRATANTE poderá solicitar aconselhamento sobre processos de melhoria, atualização ou migração das soluções para o gestor de serviços do fabricante;
g) Os relatórios dos incidentes analisados e reportados devem ser fornecidos com frequência mínima mensal para o ambiente;
h) A plataforma de investigação do serviço deve utilizar regras inteligentes com Machine Learning e Inteligência Artificial, em conjunto com a inteligência de ameaças do fabricante.

3.1.1.2 Serviço de suporte especializado para instalação, migração e suporte preventivo/corretivo:

a) Além do serviço inicial de instalação e configuração, neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução, seja este corretivo ou preventivo, bem como a transferência de conhecimento;

b) O serviço em questão deve atuar em conjunto com o suporte especializado do fabricante para atuação na manutenção e aplicação das melhores práticas no ambiente;
c) A CONTRATADA deverá prover equipe técnica especializada própria para atuar nas demandas da CONTRATANTE durante o contrato vigente.
d) Detalhamento do serviço de instalação e atualização:
a) TRENDMICRO Smart Protection Complete, TRENDMICRO workload security; e TRENDMICRO Deep Discovery;
a. Fase de Abertura:
- Validar e Homologar escopo do projeto;
- Validar objetivos e premissas do projeto;
- Validar riscos e restrições do projeto;
- Identificar e validar os requisitos do projeto;

b. Fase de Planejamento:
- Elaborar plano de projeto;
- Definir as pessoas envolvidas por parte do CONTRATANTE no projeto;
- Reunir as equipes da CONTRATADA e CONTRATANTE;
- Apresentação do cronograma do projeto com os prazos e responsabilidades;
- Verificar os pré-requisitos do projeto;
- Apresentar plano do projeto para a homologação por parte do CONTRATANTE.

c. Fase de Execução para Apex One:
- Atualização do Apex One para a versão mais nova para 100 (cem) estações de trabalho e habilitar o XDR;
- Orientar a equipe da CONTRATANTE para realizar o restante da migração;
- Redefinição da política de atualização automática.

d. Fase de execução para Apex Central:
- Atualização do Apex Central para a versão mais atualizada.
- Treinamento Hands On.

e. Fase de Execução para Application Control:
- Implantação do Application Control para a versão mais atualizada para 100 (cem) estações de trabalho;
- Orientar a equipe da CONTRATANTE para realizar o restante da migração.

f. Fase de Execução para Vulnerability Protection:
- Realização de atualização da versão do Vulnerability Protection para a versão mais atualizada para 100 (cem) estações de trabalho;
- Orientar a equipe da CONTRATANTE para realizar o restante da migração;
- Definição de política de proteção.

g. Fase de Execução para Workload Security e XDR integrado ao Vision One:
- Implantação do workload Security e XDR para 10 servidores.
- Treinamento Hands On.

h. Fase de Execução pelo Email Security Standard:
- Implantação do Email Security Standard para 1 gateway de correio eletrônico e até 2 domínios;
- Orientar a equipe da CONTRATANTE para utilização do sistema;
- Definição de política de proteção;
- Treinamento Hands On.

i. Fase de Execução do Cloud App Security (CAS) e XDR integrado ao Vision One e a sandbox;
- Implantação do Cloud App Security para 1 provedor de serviço em nuvem, integrando caixas de correio eletrônico, armazenamento em nuvem e colaboração;
- Ativação do XDR;
- Orientar a equipe da CONTRATANTE para utilização do sistema;
- Definição de política de proteção;
- Treinamento Hands On.

j. Fase de Execução para o Deep Discovery Inspector e XDR, integrado ao Vision One e sandbox:
- Instalação do Deep Discovery Inspector para a versão mais atualizada;
- Ativação do XDR para Deep Discovery Inspector para a versão mais atualizada;
- Orientar a equipe da CONTRATANTE para utilização do sistema;
- Definição de política de inspeção de rede;
- Treinamento Hands On.

k. Fase de Execução para o File Storage:
- Instalação do File Storage para a versão mais atualizada;
- Orientar a equipe da CONTRATANTE para utilização do sistema;
- Treinamento Hands On.

l. Fase de Execução para o Conformity:
- Instalação do Conformity para a versão mais atualizada;
- Orientar a equipe da CONTRATANTE para utilização do sistema;
- Treinamento Hands On.

m. Fase de Encerramento:
- Reunir as equipes CONTRATADA e CONTRATANTE para alinhamento de atividades

pendentes, caso tenha;
- Analisar e encerrar essas atividades;
- Homologar o projeto;
- Documentar as oportunidades de melhoria do processo.

3.1.1.3 Detalhamento do Serviço de Gerenciamento Proativo, Preventivo, Corretivo Especializado na solução TRENDMICRO:

a. A CONTRATADA deverá prestar suporte técnico no ambiente TRENDMICRO envolvendo as soluções de Apex One SaaS, XDR para Apex One, Apex central, Vulnerability Protection, Application Control, Workload Security, Email Security Standard, Cloud App Security, XDR para Cloud App Security, Deep Discovery Inspector, XDR para Deep Discovery Inspector, Cloud One File Storage, Cloud One Container Security, Cloud One Conformity;
b. O suporte deverá ser estar disponível na modalidade 8x5x12, remotamente e em horário comercial;
c. De acordo com a conveniência da CONTRATANTE, e a depender da complexidade do suporte necessário, a CONTRATADA poderá realizar intervenções presenciais no ambiente do Tribunal, mesmo fora do horário supracitado;
d. Os chamados de suporte que não puderem ser resolvidos diretamente pela empresa contratada devem ser escalados para o fabricante. O acompanhamento do chamado escalado para o fabricante, e a alimentação do chamado é responsabilidade da empresa contratada;
e. Deverá ser prestado um suporte proativo envolvendo as seguintes atividades:
- Diagnóstico especializado para a solução de endpoint e gateway de correio envolvendo: Apex One SaaS, Apex Central e Email Security Standard com a periodicidade anual. Esse relatório deverá verificar a conformidade das configurações das tecnologias em relação às boas práticas de mercado e as recomendações do fabricante, para orientar sobre a melhoria contínua das configurações das ferramentas de proteção;
- Diagnóstico especializado para a solução de Workload Security com a periodicidade anual. Esse relatório deverá verificar a conformidade das configurações das tecnologias em relação às boas práticas de mercado e as recomendações do fabricante, para orientar sobre a melhoria contínua das configurações das ferramentas de proteção;
- Monitoramento de Ameaças e Vulnerabilidades através do Vision One e das tecnologias integradas para 14.200 endpoints, para orientação e tomada das ações necessárias para evitar a ocorrência do incidente;
- Apresentação trimestral de indicadores e métricas de cibersegurança através do Vision One, atividade proativa que dá uma visão gerencial do ambiente cibernético e orienta a respeito de possíveis melhorias.
- Gerenciamento remoto mensal para verificação da saúde das tecnologias implantadas:
  - Vision One
  - Apex Central SaaS
  - Apex One SaaS, Vulnerability Protection, Application Control
  - Email Security Standard
  - Cloud App Security
  - Cloud ONe Workload Security
  - Deep Discovery Inspector

3.1.2 LOCAIS DE PRESTAÇÃO DOS SERVIÇOS

Os softwares estão instalados no Edifício do Tribunal de Justiça, localizado no Centro Administrativo da Bahia, e outros serviços estão alocados nos provedores de nuvem. O serviço a ser contratado será prestado de forma remota e excepcionalmente presencial, caso necessário, pelo fabricante da solução, seguindo sua política global de suporte, ou eventualmente pela CONTRATADA, nos casos em que for requerido sua intermediação junto ao fabricante.

Os técnicos da CONTRATANTE estarão disponíveis para intermediar este acesso.

3.1.3 HORÁRIOS DE PRESTAÇÃO DOS SERVIÇOS

A CONTRATADA deverá realizar os atendimentos durante o horário normal do expediente, sendo considerado, para todos os efeitos, o horário entre às 08:00 e 18:00, de segunda a sexta-feira.

Atendimentos fora do horário de expediente normal só ocorrerão mediante agendamento e de acordo anuência do CONTRATANTE /Usuário.

3.2 PRINCIPAIS PAPÉIS

a) Patrocinador da Contratação: Titular da SETIM – Secretaria de Tecnologia da Informação e Modernização, área demandante, responsável por representar os interesses do TJBA no contexto desta contratação, pela aprovação da necessidade e, por fim, pela negociação das ações necessárias para que os objetivos sejam alcançados.
b) Gerente do Contrato pelo CONTRATANTE: Servidor a ser oportunamente designado mediante portaria, em obediência ao Manual de Gerenciamento e Fiscalização de Contratos do Tribunal de Justiça, ao Decreto Judiciário nº 379 de 8 de maio de 2018 e a Norma Geral de Contratações do TJBA com as seguintes responsabilidades:
- Planejar e orientar a contratação, especialmente para estabelecer diretrizes para a contratação e condução dos vínculos contratuais.

- Manter fluxo de comunicação e administrar as relações com a CONTRATADA.
- Acompanhar o andamento do contrato, especialmente no referente aos cumprimentos e descumprimentos contratuais.
- Manter-se sempre informado de todas as ocorrências contratuais e repassar às autoridades, proativamente, aquelas que interfiram no fornecimento e/ou nos serviços.
- Paralisar a execução do contrato no caso de estar em desacordo com o pactuado ou diante de graves descumprimentos.
- Promover as pertinentes penalizações e fazer os contatos necessários em nome do Tribunal.
- Promover os pertinentes ajustes no Contrato.
- Conduzir o encerramento do Contrato.

c) Preposto da CONTRATADA: Como anexo ao contrato, deverá a CONTRATADA indicar, formalmente, o seu preposto como responsável pela execução, nos termos do art. 156, da Lei n° 9.433/05.

- O representante nomeado pela CONTRATADA deverá ter condições de coordenar a execução do contrato e ter poderes expressos para representá-la em todos os atos do contrato, especialmente para ajustes obrigacionais registrados em atas de reuniões, termos de recebimento ou recusa de objeto a ser entregue, notificações, ofícios, e demais atos relacionados à execução do contrato.
- Esta designação será escrita, assinada pelo representante da CONTRATADA (outorgante) e pelo próprio preposto indicado, devendo conter, no mínimo, as disposições do “Termo de Designação de Preposto”, anexo ao Edital.
- No ato da designação, a CONTRATADA deverá apresentar todas as informações de contato do preposto escolhido (endereço, telefone, celular, WhatsApp, e-mail, entre outros), bem como os canais específicos para o registro de solicitações, consultas, intimações, entre outros.
- Havendo necessidade de realizar reuniões de planejamento e/ou ajuste da execução dos serviços, o Gestor do Contrato poderá convocar reuniões específicas, presenciais ou remotas, às quais o Preposto da CONTRATADA deverá comparecer em data definida pelo CONTRATANTE.
- O preposto deverá, ainda:
  - Gerenciar a interação entre o CONTRATANTE e a CONTRATADA, responsabilizando-se pessoal e diretamente pela execução dos serviços contratados e pela gestão dos aspectos técnicos, administrativos, financeiros e legais do contrato.
  - Apresentar ao CONTRATANTE, mensalmente, a documentação pertinente para comprovação dos serviços e demais documentos necessários ao faturamento.
  - Responsabilizar-se pelo controle e armazenamento da documentação do contrato, bem como o registro das atas de reunião, em uma pasta da rede do CONTRATANTE, a fim de subsidiar o controle e a fiscalização do contrato.

d) Fiscais do Contrato: Servidores a serem oportunamente designados mediante portaria, em obediência ao Manual de Gerenciamento e Fiscalização de Contratos do Tribunal de Justiça, ao Decreto Judiciário nº 379, de 8 de maio de 2018 e a Norma Geral de Contratações do TJBA com as seguintes responsabilidades:

- Verificar os recursos materiais e humanos empregados na execução dos contratos.
- Verificar a forma de execução do objeto do contrato.
- Avaliar o cumprimento de todas as obrigações contratuais.
- Cobrar da CONTRATADA o cumprimento do contrato.
- Promover o registro documentado de todas as ocorrências contratuais diretamente relacionadas às obrigações assentadas no contrato.
- Manter contato com a CONTRATADA de modo a promover todo o tipo de interlocução operacional em nome do Tribunal.
- Comunicar ao gerente do contrato as ocorrências de cumprimento e de descumprimento contratual detectadas.

3.3 DINÂMICA DA EXECUÇÃO

3.3.1 CRONOGRAMA DE ENTREGA DOS SERVIÇOS

ID	Evento	Quando	Prazo em dias até	Quem
1	Assinatura do Contrato	Início	Não se aplica	Ambos
1.1	Emissão do Empenho	Após ID 1	Não se aplica	Contratante
2	Reunião de Alinhamento	Após ID 1	5 dias corridos	Ambos
3	Início do Serviço Gerenciamento mensal descrito no item 7	Após ID 2	Imediatamente	Ambos
4	Entrega dos itens de software 1,2,4, e 5	Após ID 1.1	15 dias corridos	Contratada
5	Emissão do Termo de Recebimento Definitivo (TRD) para itens 1,2,4,5	Após ID 4	10 dias corridos	Contratante

6	Entrega do *appliance* descrito no item 3	Após ID 1.1	60 dias corridos	Contratada
7	Emissão do Termo de Recebimento Definitivo (TRP) para item 3	Após ID 6	5 dias corridos	Contratante
8	Instalação física do *appliance* descrito no item 3 no Datacenter	Após ID 7	10 dias corridos	Contratada
9	Emissão do Termo de Recebimento Definitivo (TRD) para itens 3	Após ID 8	10 dias corridos	Contratante

Tabela 03

3.3.2 GERENCIAMENTO DO SERVIÇO

3.3.2.1 A CONTRATADA deverá atender aos seguintes aspectos:

- Ter como ponto focal desta atividade o Preposto da CONTRATADA estabelecido na Reunião de Alinhamento conforme o documento Modelo de Termo de Nomeação de Preposto anexo ao edital, sendo direto responsável pela prestação global da qualidade do serviço, interagindo permanentemente com os representantes do CONTRATANTE.
- Realizar o acompanhamento de cada chamado desde a sua abertura registrada CONTRATANTE e o dia / hora até o seu fechamento registrado.
- Realizar reuniões periódicas com o CONTRATANTE podendo, este último, em atenção a circunstâncias específicas, dispensar reuniões programadas ou convocar, em caso de necessidade, reuniões extraordinárias, às quais o Preposto da CONTRATADA deve comparecer no prazo máximo de dois dias úteis.
- Executar todas as atividades que nomeiem especificamente a sua responsabilidade no âmbito deste Termo de Referência.

3.3.3 ATENDIMENTO AOS CHAMADOS

Para realizar o Atendimento aos chamados, a CONTRATADA OU FABRICANTE deverá:

- Disponibilizar os canais de comunicação previstos neste TR para abertura de chamados e demais solicitações;
- Atender ao Chamado conforme os Tipos de Serviço relacionados no Item 3.5 – Nível Mínimo de Serviço, e respeitando o tempo de resolução estabelecido no mesmo tópico;
- Possuir técnicos especializados, ferramentas e equipamentos adequados, peças e componentes originais e quaisquer outros itens necessários para a boa execução dos serviços.

3.4 INSTRUMENTOS FORMAIS DE SOLICITAÇÃO

3.4.1 REUNIÃO DE ALINHAMENTO

A reunião de alinhamento, entre o CONTRATANTE e a CONTRATADA, será realizada com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no contrato, edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

Deverá ocorrer dentro do prazo máximo estabelecido no Item 3.3.1 (Cronograma de Entrega dos Serviços). Poderá ser presencial, no endereço do CONTRATANTE, ou remota por conveniência do CONTRATANTE.

Na reunião de alinhamento, CONTRATADA deverá apresentar oficialmente seu INTERLOCUTOR (Preposto ou Gerente de Contrato), designando-o mediante Termo de Designação de Preposto, cujo modelo segue anexo ao edital.

3.4.2 SOLICITAÇÕES

Os serviços serão solicitados pelo CONTRATANTE por meio de registro de chamado através de contato telefônico, ligação gratuita (0800), e-mail (correio eletrônico) ou através de ferramenta de registro de chamados da CONTRATADA, por procedimentos específicos, com controle de acesso por senha, em consonância com as definições feitas no item 3.1.1 (Serviços a Serem Executados Pela Contratada).

3.5 ACOMPANHAMENTO DOS PRAZOS DE GARANTIA E NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

3.5.1 Quanto à garantia e suporte a serem prestados pelo FABRICANTE

Considerando que a presente demanda se refere à contratação de Serviços com níveis predefinidos pelo fabricante, o Nível Mínimo de Serviço exigido para essa categoria de serviços será baseado no compromisso de qualidade e de prazos definidos no modelo “Trend Micro™ Premium Support”, definida na Política de Suporte do fabricante da solução[7] .

7 www.trendmicro.com/pt_br/business/products/support-services.html?modal=6b5bce

3.5.2 Quanto ao serviço de gerenciamento especializado, proativo, preventivo e corretivo, a ser prestado pela contratada (Item 7)

Para os serviços constantes no item 7 – Gerenciamento especializado, proativo, preventivo e corretivo de ameaças, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

Níveis de severidade do incidente	
Nível	**Descrição**
Alto	Serviços indisponíveis com alto impacto em processos de negócio
Médio	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta aos processos de negócio
Baixo	Serviços disponíveis com ocorrência de alertas e avisos sobre eventuais problemas, dúvidas gerais sobre as soluções fornecidas.

Tabela 04

Prazos	**Níveis de severidade**		
	Alto	**Médio**	**Baixo**
Início do atendimento	4 horas	8 horas	12 horas

Tabela 05

Os serviços de suporte serão prestados por profissionais designados pela CONTRATADA, no horário das 08hs às 18hs, de segunda a sexta-feira, em dias úteis, preferencialmente de forma remota.

O chamado de suporte poderá ser aberto por e-mail, telefone ou por aplicação própria da CONTRATADA

Todo chamado de suporte deverá gerar um relatório de atendimento técnico, relativo ao problema ocorrido, que deverá fazer parte da entrega mensal da Contratada.

A empresa CONTRATADA compromete-se a manter registros de todos os chamados, incluindo transcrição das interações técnicas, constando o nome do técnico da empresa e uma descrição resumida do incidente/problema, disponibilizando-os ao TJBA quando solicitado.

Quaisquer alegações, por parte da CONTRATADA contra instalações (ambiente inadequado, rede elétrica etc.) ou usuários (mau uso etc.) do TJBA, devem ser comprovadas tecnicamente através de pareceres, os quais deverão ser homologados e reconhecidos pelo TJBA.

3.5.3 A cada mês a Contratada deverá entregar ou realizar:

1) Relatório de atendimento técnico de cada solicitação aberta no suporte;
2) Relatório sumarizado de atendimentos, contendo a data e hora de abertura e início de atendimento das solicitações, e duração total de cada atendimento, indicando o quantitativo de atendimentos violados e o total em minutos de violação para cada nível de severidade;
3) Relatório sumarizado mensal de notificações do monitoramento de ameaças digitais e vulnerabilidades;
4) Relatório mensal de saúde das ferramentas monitoradas;
5) Reunião gerencial de acompanhamento mensal do serviço de gerenciamento, para apresentação dos entregáveis descritos;
6) Ata de Reunião Mensal;

A reunião gerencial deverá ocorrer até o 5º dia útil do mês subsequente à prestação dos serviços. A ata resultante da reunião servirá como instrumento formal da entrega do serviço prestado.

Os documentos relacionados acima terão validade legal para fins de aferição de resultados, comprovação, contestação, entre outros.

3.6 INSTRUMENTOS DE MEDIÇÃO DOS SERVIÇOS

O desempenho do serviço de Gerenciamento especializado, proativo, preventivo e corretivo de ameaças (Item 7 da solução), será verificado através da tabela a seguir, onde cada ponto representa 0,5% de glosa, até o limite de 20%.

ITEM	Termo de Serviços	Referência	Pontuação
TS01	Deixar de enviar os relatórios de atendimento técnico sobre o gerenciamento remoto das soluções	Por chamado aberto	5
TS02	Deixar de enviar a notificação do monitoramento de ameaças digitais e vulnerabilidades de alto risco	Por evento	5
TS03	Deixar de enviar a ata da reunião de acompanhamento das entregas do contrato	Por reunião ocorrida	5
TS04	Violação de prazo para início de atendimento para solicitações de severidade baixa	A cada hora violada	2
TS05	Violação de prazo para início de atendimento para solicitações de severidade média	A cada hora violada	4
TS06	Violação de prazo para início de atendimento para solicitações de severidade alta	A cada hora violada	6

Tabela 06

Ao final de cada mês, será calculado o somatório total da pontuação por cada evento de termo de serviço violado. O somatório será multiplicado por 0,5% para se obter o indicador GL.

Portanto, têm-se que:

VD = VF- GL

Onde:
VD = Valor Devido do Serviço
VF = Valor Fixo do Serviço
GL = Glosa de Serviços (%)

3.7 ACOMPANHAMENTO DA EXECUÇÃO

O preposto, indicado pela CONTRATADA como seu representante na reunião de alinhamento, será o responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, administrativas e outras correlatas, referentes ao andamento contratual. Este serviço, de gerenciamento do contrato e dos diversos serviços nele contemplados, será prestado sem ônus específico.

Pela parte do CONTRATANTE, as decisões operacionais serão tomadas pela Diretoria de Informática através da Coordenação de Suporte Técnico – COTEC, que fiscalizará a execução e realizará as notificações pertinentes, podendo exigir da CONTRATADA, a qualquer tempo, esclarecimentos, demonstrações e documentos que comprovem a regularidade do contrato.

Toda a coordenação técnica dos e administrativa (planejamento dos serviços, logística de execução, controle da frequência dos técnicos, cumprimento de férias e demais obrigações trabalhistas etc.) será responsabilidade do Preposto da CONTRATADA.

3.8 RECEBIMENTO PROVISÓRIO E DEFINITIVO

O TJBA designará servidor responsável para realizar o recebimento dos objetos, da seguinte forma:

3.8.1 Termo de Recebimento Provisório

Para os itens de hardware: Deverão ser comprovadas as entregas desses objetos nas dependências do TJBA, no prazo definido no item 3.3.1 - cronograma de entrega dos serviços.
Todas as comprovações serão aceitas em formato digital ou impresso, via e-mail ou presencialmente.

3.8.2 Termo de Recebimento Definitivo

Os Termos de Recebimento Definitivo serão emitidos conforme a seguir:

Para os itens de Software: Os objetos deverão ser entregues através de carta emitida pelo fabricante contendo as informações dos objetos contratados, o regime de suporte especificado no termo de referência, os dados de acesso do

TJBA ao portal de suporte do fabricante, a vigência dos serviços contratados, os dados do cliente e do fabricante, e registro informativo de que os produtos foram adquiridos através do licitante arrematante.

Para os itens de Hardware: Os objetos deverão ser instalados fisicamente no Datacenter, na sede do TJBA.

Para os itens de treinamento: Será atestado o recebimento dos itens em até 10 (dez) dias corridos, após a realização dos treinamentos previstos nesta contratação.

Para os itens de prestação de serviços: Serão emitidos mensalmente, após cumpridos os requisitos descritos nos itens 3.5 (Acompanhamento dos Prazos de Garantia e Níveis Mínimos de Serviço), 3.6 (Instrumentos de Medição dos Serviços) e seus subitens.

Os **Termos de Recebimento Definitivo**, nos termos do Art. 161 da Lei Estadual nº 9.433/2005, serão emitidos em razão de parecer circunstanciado de servidor ou comissão designada pela autoridade competente, mediante termo assinado pelas partes, após as entregas das atividades descritas neste item, nos prazos indicados no item 3.3.1 – Cronograma de Entrega dos Serviços.

A emissão de aceite dos serviços pelo CONTRATANTE não exime a CONTRATADA da responsabilidade pela correção de erros porventura identificados, sem ônus adicional.

3.9 FORMA DE PAGAMENTO

O faturamento só poderá ser apresentado após a emissão do Termo de Recebimento Definitivo (TRD), indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao fornecimento e prestação dos serviços, acompanhado da documentação probatória relativa ao recolhimento dos impostos relacionados com a obrigação, obedecidos os prazos descritos no **item 3.3.1 – Cronograma de Entrega dos Serviços.**

Devido à política global de venda do fabricante, para os itens de 01 a 05, componentes da solução, o pagamento será efetuado em parcela única após Termo de Recebimento Definitivo a ser emitido para cada um dos itens.

Para o item 06 da solução, que ocorrerá sob demanda, o faturamento também será feito em parcela única, de acordo com o consumo, e só poderá ser apresentado após a CONTRATANTE emitir o TRD do respectivo item, indicando a realização e satisfação com os treinamentos entregues;

Para o item 07 da solução, o pagamento será realizado mensalmente, após verificados os critérios descritos nos itens 3.5 (Acompanhamento dos Prazos de Garantia e Níveis Mínimos de Serviço) e 3.6 (Instrumentos de Medição dos Serviços). Deverá ser apresentada uma Nota Fiscal para cada mês de serviço prestado.

Os faturamentos deverão ser apresentados em notas fiscais de venda ou serviço, de acordo com as características de cada objeto, e serão pagos através de ordem bancária ou crédito em conta corrente, em até 08 (oito) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, condicionado ao seu ateste pelo Gestor do Contrato, em consonância com o disposto no art. 6º, § 5º; art. 8º, XXXIV; art. 79, XI, “a”; art. 154, V e art. 155, V da Lei Estadual nº 9.433/05.

O valor global a ser pago à CONTRATADA deverá atender aos valores cotados na proposta vencedora.

A efetivação e aceite de quaisquer serviços não previstos só poderão ocorrer mediante aprovação formal do CONTRATANTE.

3.10 TRANSIÇÃO CONTRATUAL

Durante a vigência do contrato, caberá à CONTRATADA realizar a transferência de conhecimento de modo tácito ou explícito com objetivo de disseminar a informação referente às questões técnicas implementadas no ambiente operacional do CONTRATANTE.

Os meios utilizados para essa transferência serão previamente acordados entre CONTRATADA e CONTRATANTE, podendo consistir em um ou uma combinação dos seguintes meios:

- Divulgação eletrônica;
- Base de conhecimentos;
- Registro de lições aprendidas;
- Registro de soluções alternativas utilizadas;
- Registro de ocorrências, conhecimentos e procedimentos relacionados a cada sistema;
- Documentação de melhores práticas;
- Reuniões e suas respectivas atas;
- Relatórios periódicos;
- Ferramentas de comunicação em geral: videoconferência, chat, e-mail.

3.10.1 TRANSFERÊNCIA FINAL DE CONHECIMENTO

Ao final deste contrato a CONTRATADA deve, em conformidade com o parágrafo único do artigo 111 da Lei nº 8.666/93, promover transição contratual e repassar para o CONTRATANTE e/ou para a nova contratada todos os dados, documentos e elementos de informação utilizados na execução dos serviços.

3.10.1.1 Passagem de Serviço

Não se aplica a esta contratação. Entretanto, a equipe de gestão do contrato deverá ficar atenta ao prazo de vigência dos serviços para que sejam contratados, em tempo hábil, novos pacotes de forma que não haja descontinuidade na prestação dos serviços de suporte e atualização das versões.

3.10.1.2 Devolução de recursos materiais

Não se aplica a essa contratação.

3.10.1.3 Revogação de perfis de acesso

Ao término do contrato, serão revogados todos os perfis de acesso eventualmente concedidos a técnicos da CONTRATADA.

3.10.1.4 Eliminação de caixas postais

Ao término do contrato, serão eliminadas eventuais contas de e-mail de profissionais da CONTRATADA.

3.10.2 ENCERRAMENTO ABRUPTO DO CONTRATO

Tratando o presente processo da contratação única e global, não há expectativa de descontinuidade no fornecimento, exceto a hipótese de descumprimento contratual, situação em que serão aplicadas as penalidades cabíveis.

Em caso de encerramento abrupto do contrato deverá ser iniciado, de imediato, o planejamento de nova contratação.

3.11 DIREITOS DE PROPRIEDADE INTELECTUAL

Todas as atividades, documentação e produtos desenvolvidos durante a execução dos serviços serão de propriedade única e exclusiva do CONTRATANTE.

A CONTRATADA deverá entregar ao CONTRATANTE toda e qualquer documentação gerada em função da prestação de serviços, objeto da contratação. Entende-se por documentação quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, fontes dos códigos dos programas em qualquer mídia, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

A CONTRATADA fica proibida de comercializar os produtos relativos ao objeto da prestação dos serviços, ficando sujeita às penalidades previstas na Lei 9.609/98 em caso de descumprimento desta determinação.

Os direitos autorais dos serviços técnicos serão de exclusividade do CONTRATANTE, que poderá publicar e/ou divulgar seus resultados, quando considerados pertinentes.

A utilização de soluções ou componentes proprietários da CONTRATADA ou de terceiros na execução dos serviços relacionados ao presente contrato, que possam afetar a propriedade do produto, deve ser formal e previamente autorizada pelo TJBA.

3.12 QUALIFICAÇÃO TÉCNICA PROFISSIONAL

A composição da equipe técnica deverá ser provida e dimensionada pela CONTRATADA, estabelecendo adequada relação entre a quantidade e produtividade individual dos profissionais por ela disponibilizados e o prazo contratual, assumindo toda a responsabilidade trabalhista e de normas de segurança do trabalho, além dos impostos e tributos aplicáveis. Estes profissionais deverão dispor de ferramentas e insumos necessários e suficientes à execução dos serviços.

No início dos serviços, na reunião de alinhamento, a Contratada deverá apresentar a comprovação da qualificação técnica exigida no **item 4.10 - Requisitos da Contratada**.

3.13 GARANTIA CONTRATUAL

Em garantia de plena, fiel e segura execução de tudo o que se há obrigado, a CONTRATADA prestará caução correspondente a 5% (cinco por cento) sobre o valor global do objeto contratado, em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, cuja liberação ou restituição dar-se-á após a expiração deste instrumento contratual.

A garantia será obrigatoriamente revista e complementada quando houver redução da sua representatividade percentual por variação econômica do contrato ou descontos de valores devidos ao CONTRATANTE, a exemplo de multas, quando for o caso.

A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais.

O cálculo da atualização monetária do valor caucionado em dinheiro será feito aplicando-se o índice mais vantajoso para a Administração entre a data de retenção da caução e da devolução do seu valor.

A garantia deverá ser apresentada no prazo máximo de 10 (dez) dias corridos, contados da assinatura do Contrato.

3.14 DESCUMPRIMENTO DAS OBRIGAÇÕES CONTRATUAIS

Com fundamento nas Leis Federais nº 8.666/1993 e nº 10.520/2002, na Lei Estadual nº 9.433/2005, e nos Decretos do Poder Judiciário do Estado da Bahia nº 12/2003 e nº 44/2003, a CONTRATADA que incorrer em ilícitos ou faltas administrativas ficará sujeita, além das sanções previstas em Contrato no caso de descumprimento das obrigações pactuadas, às sanções previstas na referida Lei Estadual, sem prejuízo das responsabilidades civil e criminal, assegurada prévia e ampla defesa.

As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

As multas não impedem que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas em lei, bem como não têm caráter compensatório e o seu pagamento não eximirá a CONTRATADA da responsabilidade por perdas e danos decorrentes das infrações cometidas.

Para a aplicação das penalidades previstas, será levada em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato.

Outras sanções poderão eventualmente ser impostas à CONTRATADA de acordo com a legislação aplicável.

4 REQUISITOS TÉCNICOS ESPECÍFICOS

4.1. SOLUÇÃO DE SEGURANÇA – Sistemas Críticos com Proteção para Cargas de trabalho e Visibilidade de Perímetro

4.1.1. Os requisitos de fornecimento, instalação e garantia dos materiais e ou softwares descritos abaixo deverão obedecer aos itens e subitens deste Termo de Referência;
4.1.2. As especificações de serviços, características técnicas e quantidades mínimas especificadas neste Anexo são de caráter obrigatório;
4.1.3. Para atender a integridade da solução e facilitar a gestão do ambiente, todas as soluções devem ser do mesmo fabricante;
4.1.4. As soluções poderão, dependendo do escopo, ser entregues como serviço (nuvem) ou local (on-premises).

4.2. COMPOSIÇÃO DA SOLUÇÃO

ID	TÓPICO	ITEM	DESCRIÇÃO DO ITEM	Part Number	QTD.
1	4.3	Software de segurança para usuário final, contendo ambiente isolado e seguro para teste de novas ameaças, com visibilidade, detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Smart Protection Complete com detecção e resposta – 24 meses meses	CTNA0045 CTRA0045	14.200
			Apex One Sandbox as a Service Add-on to Apex One – 24 meses – 24 meses	ADNA0018 ADRA0015	
			Vision One XDR- 24 meses	VONA0000	
2	4.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One - Workload Security with XDR – 24 meses	CXNI0004 CXRI0004	1.001
			Service One Complete endpoint e Workload– 24 meses	SYNN0012 SYRN0012	
3	4.5	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante 24 (vinte e quatro) meses.	Deep Discovery Inspector Series 4000: 4Gbps SW+HW Appliance – 24 meses Deep Discovery Inspector 4000 Series Hardware	DDNA0033 DDRA0029 DDNA0019	1
			Vision One XDR- 24 meses	VONA0000	
			Service One Complete Network– 24 meses	SYN30000 SYR30000	
4	4.6	Solução de proteção para serviços em nuvem com validação de melhores práticas, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One Conformity – 24 meses	CXNA0048 CXRA0048	10
5	4.7	Solução de proteção para áreas de armazenamento de arquivos em nuvem, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One File Storage Security per bucket/blob- 24 meses	CXNA0027 CXRA0027	10
6	4.8	Treinamento oficial do fabricante	Voucher de Treinamento Oficial	TRNN1041	6
7	4.9	Gerenciamento especializado, proativo, preventivo e corretivo de ameaças por 24 (vinte e quatro) meses	Serviço de suporte especializado para diagnósticos, ajustes, configurações, migrações e implementação da solução a ser fornecida	Serviço Mensal	24

Os Part Numbers aqui listados servem como referência dos produtos a serem fornecidos. Caso os part numbers dos produtos tenham sidos alterados pelo fabricante, deverá ser apresentado documento oficial do fabricante comprovando esta alteração.

4.3. SOFTWARE DE SEGURANÇA PARA USUÁRIO FINAL, CONTENDO AMBIENTE ISOLADO E SEGURO PARA TESTE DE NOVAS AMEAÇAS, COM VISIBILIDADE, DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO POR 24 MESES

4.3.1. Características gerais

4.3.1.1. A solução deverá ser entregue na modalidade on-premises (local) ou como um serviço (em nuvem);

4.3.1.2. Possuir console Web para gerenciamento e administração da ferramenta;

4.3.1.3. A solução deverá ser toda de um único fabricante;

4.3.1.4. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações, Controle de dispositivos e EDR (Endpoint Detection and Response) em um único agente.

4.3.2. Módulo de Proteção Anti-Malware

4.3.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.3.2.1.1. Windows 8.1 (x86/x64);

4.3.2.1.2. Windows 10 (x86/x64);

4.3.2.1.3. Windows 11 (x64).

4.3.2.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

4.3.2.3. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

4.3.2.4. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

4.3.2.4.1. Processos em execução em memória principal (RAM);

4.3.2.4.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

4.3.2.4.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

4.3.2.4.4. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

4.3.2.5. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;
4.3.2.6. Deve possuir detecção heurística de vírus desconhecidos;
4.3.2.7. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;
4.3.2.8. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):
4.3.2.8.1. Em tempo real de arquivos acessados pelo usuário;
4.3.2.8.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
4.3.2.8.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;
4.3.2.8.4. Automáticos do sistema com as seguintes opções:
4.3.2.8.4.1. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
4.3.2.8.4.2. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
4.3.2.8.4.3. Frequência: horária, diária, semanal e mensal;
4.3.2.8.4.4. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;
4.3.2.9. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;
4.3.2.10. Em caso de arquivos suspeitos, a solução deve ter a capacidade de enviar o artefato para um ambiente de sandbox do próprio fabricante para identificar ameaças desconhecidas;
4.3.2.11. O módulo de análise de artefatos desconhecidos (sandbox) deve estar integrada à solução de antimalware, sem necessidade de plugins adicionais;
4.3.2.12. O módulo de sandbox deve permitir a análise de arquivos submetidos diretamente dos agentes;
4.3.2.13. Em caso de ameaças desconhecidas detectadas pela sandbox, a solução deve ter a capacidade de adicionar os objetos suspeitos (hash de arquivo, IP, domínio e URL) numa lista de bloqueio automaticamente;
4.3.2.14. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
4.3.2.15. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;
4.3.2.16. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URLs maliciosas, de modo a prover, rápida detecção de novas ameaças;
4.3.2.17. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;
4.3.2.18. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;
4.3.2.19. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos
4.3.2.20. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;
4.3.2.21. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;
4.3.2.22. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;
4.3.2.23. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;
4.3.2.24. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;
4.3.2.25. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;
4.3.2.26. Deve bloquear processos comuns associados a ransomware;
4.3.2.27. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios;
4.3.2.28. Deve possuir funcionalidade de detecção de Malware conhecidos e desconhecidos por comportamento;
4.3.2.29. Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

4.3.3. Funcionalidade de Atualização

4.3.3.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
4.3.3.2. Deve permitir atualização incremental da lista de definições de vírus;
4.3.3.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;
4.3.3.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engine;

4.3.3.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de antimalware para essas tarefas;
4.3.3.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;
4.3.3.7. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

4.3.4. Funcionalidade de Administração
4.3.4.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
4.3.4.2. Deve possibilitar instalação "silenciosa";
4.3.4.3. Deve permitir o bloqueio por nome de arquivo;
4.3.4.4. Deve permitir o travamento de pastas e diretórios;
4.3.4.5. Deve permitir o travamento de compartilhamentos;
4.3.4.6. Deve permitir o rastreamento e bloqueio de infecções;
4.3.4.7. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
4.3.4.8. Quando on-premises, deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
4.3.4.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
4.3.4.10. Deve permitir a desinstalação através da console de gerenciamento da solução;
4.3.4.11. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
4.3.4.12. Quando on-premises, deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;
4.3.4.13. Deve permitir a deleção dos arquivos quarentenados;
4.3.4.14. Deve permitir remoção automática de clientes inativos por determinado período de tempo;
4.3.4.15. Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;
4.3.4.16. Quando on-premises, identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada. Em caso de soluções em nuvem, será aceita utilização de ferramenta do próprio fabricante para varredura local;
4.3.4.17. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
4.3.4.18. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
4.3.4.19. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
4.3.4.20. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory, tipo ou IP;
4.3.4.21. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;
4.3.4.22. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
4.3.4.23. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;
4.3.4.24. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;
4.3.4.25. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;
4.3.4.26. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;
4.3.4.27. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;
4.3.4.28. Deve permitir a criação de usuários locais de administração da console de anti-malware;
4.3.4.29. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;
4.3.4.30. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;
4.3.4.31. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;
4.3.4.32. Deve permitir a gerência de domínios separados para usuários previamente definidos;
4.3.4.33. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio

definido na console de administração;
4.3.4.34. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

4.3.5. Funcionalidade de Controle de Dispositivos
4.3.5.1. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;
4.3.5.2. Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);
4.3.5.3. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;
4.3.5.4. Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
4.3.5.5. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;
4.3.5.6. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
4.3.5.7. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;
4.3.5.8. Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;
4.3.5.9. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;
4.3.5.10. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

4.3.6. Módulo de Proteção Anti-Malware para estações MacOS

4.3.6.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:
4.3.6.1.1. macOS 12 (Monterey);
4.3.6.1.2. macOS 11 (Big Sur)
4.3.6.1.3. macOS 10.15 (Catalina);
4.3.6.1.4. macOS 10.14 (Mojave);
4.3.6.1.5. macOS 10.13 (High Sierra);
4.3.6.2. Suporte ao Apple Remote Desktop para instalação remota da solução;
4.3.6.3. Gerenciamento integrado à console de gerência central da solução
4.3.6.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;
4.3.6.5. Permitir a verificação das ameaças da maneira manual e agendada;
4.3.6.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;
4.3.6.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;
4.3.6.8. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;
4.3.6.9. Deve possuir no mecanismo de autoproteção as seguintes proteções:
4.3.6.9.1. Proteção e verificação dos arquivos de assinatura;
4.3.6.9.2. Proteção dos processos do agente de segurança;
4.3.6.9.3. Proteção das chaves de registro do agente de segurança;
4.3.6.9.4. Proteção do diretório de instalação do agente de segurança.

4.3.7. Funcionalidade de HIPS – Host IPS e Host Firewall
4.3.7.1. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:
4.3.7.1.1. Windows 8.1 (x86/x64);
4.3.7.1.2. Windows 10 (x86/x64);
4.3.7.1.3. Windows 11 (x64).
4.3.7.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;
4.3.7.3. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;
4.3.7.4. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);
4.3.7.5. Deve permitir ativar e desativar o produto sem a necessidade de remoção;
4.3.7.6. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;
4.3.7.7. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;
4.3.7.8. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;
4.3.7.9. O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;
4.3.7.10. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra

ameaças conhecidas ou desconhecidas;
4.3.7.11. O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;
4.3.7.12. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;
4.3.7.13. Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;
4.3.7.14. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

4.3.8. Módulo para Controle De Aplicações

4.3.8.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
4.3.8.1.1. Windows 8.1 (x86/x64);
4.3.8.1.2. Windows 10 (x64);
4.3.8.1.3. Windows 11 (x64);
4.3.8.2. As regras de controle de aplicação devem permitir as seguintes ações:
4.3.8.2.1. Permissão de execução;
4.3.8.2.2. Bloqueio de execução;
4.3.8.2.3. Bloqueio de novas instalações.
4.3.8.3. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,
4.3.8.4. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;
4.3.8.5. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:
4.3.8.5.1. Assinatura SHA-1 e SHA-256 do executável;
4.3.8.5.2. Atributos do certificado utilizado para assinatura digital do executável;
4.3.8.5.3. Caminho lógico do executável;
4.3.8.5.4. Base de assinaturas de certificados digitais válidos e seguros.
4.3.8.6. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;
4.3.8.7. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;
4.3.8.8. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;
4.3.8.9. Deve permitir a busca por aplicações ou fabricante destas;
4.3.8.10. Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

4.3.9. Módulo de Detecção e Resposta

4.3.9.1. A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;
4.3.9.2. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;
4.3.9.3. A solução deve possuir módulo de investigação e detecção integrados;
4.3.9.4. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;
4.3.9.5. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;
4.3.9.6. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
4.3.9.7. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;
4.3.9.8. Ter a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;
4.3.9.9. Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;
4.3.9.10. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;
4.3.9.11. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;
4.3.9.12. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;
4.3.9.13. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
4.3.9.14. Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
4.3.9.15. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

4.3.9.16. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
4.3.9.17. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;
4.3.9.18. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
4.3.9.19. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
4.3.9.20. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
4.3.9.21. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;
4.3.9.22. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
4.3.9.23. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;
4.3.9.24. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
4.3.9.25. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
4.3.9.26. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;
4.3.9.27. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;
4.3.9.28. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
4.3.9.29. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;
4.3.9.30. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
4.3.9.31. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
4.3.9.32. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
4.3.9.33. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;
4.3.9.34. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;
4.3.9.35. Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;
4.3.9.36. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;
4.3.9.37. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;
4.3.9.38. Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;
4.3.9.39. Permitir coletar e fazer o download de um arquivo para investigação local detalhada;
4.3.9.40. Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;
4.3.9.41. Restaurar a conectividade da estação de trabalho com a rede;
4.3.9.42. Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;
4.3.9.43. Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

4.3.10. Funcionalidade de Criptografia de disco:

4.3.10.1. Possuir a capacidade de realizar a criptografia nos seguintes sistemas operacionais:
4.3.10.1.1. Windows 8.1 (x86/x64) e;
4.3.10.1.2. Windows 10 (x86/x64).
4.3.10.2. Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para: Disco completo (FDE – full disk encryption); Pastas e arquivos; Mídias removíveis; Anexos de e-mails e Automática de disco;
4.3.10.3. Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;
4.3.10.4. Possuir a capacidade de exceções para criptografia automática;
4.3.10.5. Possuir compatibilidade de autenticação por múltiplos fatores;
4.3.10.6. Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;
4.3.10.7. Possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;
4.3.10.8. Possuir mecanismos para wipe (limpeza) remoto;
4.3.10.9. Possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);
4.3.10.10. Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;
4.3.10.11. O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);
4.3.10.12. Permitir, em nível de política, a indicação de pastas a serem criptografadas;

4.3.10.13. Possibilitar que cada política tenha uma chave de criptografia única;
4.3.10.14. Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;
4.3.10.15. Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;
4.3.10.16. Possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação.

4.3.11. Módulo de proteção para smartphones e tablets

4.3.11.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:
4.3.11.1.1. IOS e Android;
4.3.11.2. As funcionalidades estarão disponíveis de acordo com cada plataforma
4.3.11.3. Deve permitir o provisionamento de configurações de:
4.3.11.3.1. Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;
4.3.11.4. Deve possuir proteção de anti-malware para Android;
4.3.11.5. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;
4.3.11.6. Possuir capacidade de detecção de spam proveniente de SMS;
4.3.11.7. Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;
4.3.11.8. Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;
4.3.11.9. Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas;
4.3.11.10. Permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;
4.3.11.11. Permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;
4.3.11.12. Possuir controle da política de segurança de senhas, com critérios mínimos de: Padrão de senha; Uso obrigatório de senha; Tamanho mínimo; Tempo de expiração; Bloqueio automático da tela; Bloqueio por tentativas inválidas.
4.3.11.13. Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:
4.3.11.14. Bluetooth;
4.3.11.15. Câmera;
4.3.11.16. Cartões de memória;
4.3.11.17. Wlan/wifi;
4.3.11.18. GPS;
4.3.11.19. Microsoft Activesync;
4.3.11.20. MMS/SMS;
4.3.11.21. Alto-falante;
4.3.11.22. Armazenamento USB;
4.3.11.23. 3G;
4.3.11.24. Modo de desenvolvedor;
4.3.11.25. Ancoragem (tethering).

4.3.12. Proteção avançada com filtro de conteúdo para navegação web

4.3.12.1. Características gerais
4.3.12.1.1. A solução deve ser capaz de detectar malware conhecido e desconhecido;
4.3.12.1.2. As assinaturas e inteligência utilizadas pela solução devem pertencer ao mesmo fabricante da solução;
4.3.12.1.3. A funcionalidade de antimalware deve estar contida no licenciado fornecido, sem necessidade de taxas ou licenciamento adicional;
4.3.12.1.4. Não serão aceitas combinações com soluções open-source como Squid;
4.3.12.1.5. A solução deve ser capaz de detectar documentos exploráveis. Deve incluir suporte para tipos de arquivos do Microsoft Office e PDF. Todas as explorações críticas baseadas em CVE nesses arquivos devem ser detectadas;
4.3.12.1.6. A solução deve ser capaz de detectar e bloquear malware desconhecido (não baseado em assinaturas) em tempo real de acordo com funcionalidade de Machine Learning;
4.3.12.1.7. Deve ser compatível com arquivos Windows PE;
4.3.12.1.8. O arquivo suspeito pode ser bloqueado de acordo com a ação definida logo na primeira conexão;
4.3.12.1.9. A solução deve ser capaz de detectar botnet com URLs e IPs;
4.3.12.1.10. A solução deve ser capaz de detectar sites maliciosos através de mecanismos pela pontuação/classificação;
4.3.12.1.11. A solução deve ser capaz de bloquear sites maliciosos por "categoria web". O requisito mínimo de categoria deve incluir: Ransomware, Phishing, Scam, Spam, C&C, Vetor de doença (site de malware conhecido) e conexões IOT inseguras (detecção de botnet IoT);
4.3.12.1.12. "A solução deve ser capaz de detectar e bloquear conteúdo por tipo de arquivo verdadeiro (true file type) como política de usuário/grupo;

4.3.12.1.13. Deve suportar a configuração da ação por política;
4.3.12.1.14. Deve ser compatível com os seguintes tipos de arquivos: EPS, CHM, GZ, RAR, SIT, TAR, ZIP, AIF, FLV, M4A, MID, MOV, MP4, MP3, RA/RM, SWF, WAV, AVI, ASF, COM, DLL, EXE, LNK, MSI, BMP, GIF, JPG, PNG, PSD, PSP, TIF, DOC/X, ODT, PDF, PPT/X, WPD, XLS/X;
4.3.12.1.15. A solução deve oferecer suporte à filtragem de URL para restringir o acesso dos usuários por categoria da web;
4.3.12.1.16. A solução deve oferecer suporte a pelo menos 85 categorias da web para filtragem de URL;
4.3.12.1.17. A solução deve suportar o controle de, pelo menos, 700 aplicações distintas;
4.3.12.1.18. O mecanismo de controle de aplicações deve permitir a configuração das ações por política, tendo, pelo menos, as ações de Bloquear e Permitir;
4.3.12.1.19. A solução deve ser capaz de restringir o acesso da conta "pessoal" (não assinada pela empresa) aos serviços abaixo. Google G-Suite, Microsoft Office 365, Microsoft Azure e Dropbox;
4.3.12.1.20. A solução deve ser capaz de configurar a política com base em:
4.3.12.1.20.1. (Diretório / Domínio) usuário ou grupo
4.3.12.1.20.2. Gateway (local, breakout) e opção de exceção com endereço IP
4.3.12.1.20.3. Tipo de tráfego (categoria de filtragem de URL, controle de aplicativos, aplicativo em nuvem;
4.3.12.1.20.4. Tipo de arquivo (MIME, True Filetype ou nome de arquivo);
4.3.12.1.20.5. Agendamento de horários;
4.3.12.1.20.6. Ação: Bloquear e Permitir.
4.3.12.1.21. A solução deve ser capaz de configurar listas de permissão ou bloqueio em escopo globais;
4.3.12.1.22. A solução deve ser capaz de descriptografar o tráfego HTTPS;
4.3.12.1.23. A solução deve ser capaz de importar CA de raiz intermediária para descriptografias HTTPS;
4.3.12.1.24. A solução deve ser capaz de tomar ação quando uma comunicação com uma CA falhar na validação. Em caso de falha, deve incluir a CA como não confiável, CA expirada. A ação deve incluir Bloquear, Permitir;
4.3.12.1.25. A solução deve ser capaz de executar a função de túnel automático. Enquanto qualquer um dos servidores falhar, a 2ª conexão deve ser auto-tunelada por causa do erro do lado do servidor;
4.3.12.1.26. A solução deve ser capaz de registrar o domínio principal do site autotunelado;
4.3.12.1.27. A solução deve ser capaz de permitir que o administrador verifique o site com túnel automático, esse administrador deve ser capaz de configurar a política para esses sites com túnel como de "continuar túnel" ou "não-túnel automático";
4.3.12.1.28. A solução deve ser capaz de oferecer suporte a várias CA raiz para descriptografia HTTPS na política;
4.3.12.1.29. A solução deve ser capaz de configurar a política para descriptografar o tráfego HTTPS para, pelo menos, 85 categorias da web;
4.3.12.1.30. A solução deve ser capaz de gerenciar todas as políticas na nuvem e no proxy local em uma única console. O gerenciamento da política deve ser realizado via console de gerenciamento baseado em GUI não deve ser realizado como baseado em comando (por exemplo, CLI, SSH);
4.3.12.1.31. A solução deve ser capaz de definir o PAC em um console. O PAC deve ser editável por meio do console de gerenciamento baseado em GUI;
4.3.12.1.32. Os meios para análise do tráfego devem incluir, pelo menos, arquivo PAC configurado nos browsers e agente para forçar o direcionamento do tráfego para o gateway web;
4.3.12.1.33. Deve ter a capacidade de filtrar tráfego de dispositivos móveis através de VPN configurada para direcionar o tráfego para o gateway web;
4.3.12.1.34. A solução deve ser capaz de configurar várias contas de administrador;
4.3.12.1.35. A solução deve ser capaz de mostrar as estatísticas dos últimos 7 dias no painel;
4.3.12.1.36. A solução deve ser capaz de realizar análises de log para violações;
4.3.12.1.37. O dashboard deve exibir, tendo a opção de customizar o tempo, pelo menos: estatísticas de tráfego por tamanho, detecções de malware, categorias de URLs detectadas, aplicações detectadas, tráfego por localidade;
4.3.12.1.38. O dashboard deve permitir a personalização dos dados para exibir, pelo menos, gráficos de barra, tabelas e gráfico de pizza;
4.3.12.1.39. O dashboard deve permitir customização dos componentes exibidos, permitindo sua inclusão e exclusão, de acordo com a necessidade do administrador;
4.3.12.1.40. A solução deve permitir incluir gateways por localidade para que a classificação do tráfego possa ser feita localmente. Nos casos de usuários em trabalho remoto, o tráfego deve ser identificado pelo IP de origem, bem como pelo usuário que está navegando;
4.3.12.1.41. A solução deve permitir a criação de categorias personalizadas de sites, com os quais o administrador possa utilizá-las nas políticas de acesso;
4.3.12.1.42. Deve permitir a personalização das notificações enviadas para os usuários contendo, pelo menos, as seguintes notificações: bloqueio de acesso por política, bloqueio de acesso por URL maliciosa, aviso de acesso ilegal, regras de bypass através de senha, detecção de ameaças, falha de validação de certificado;
4.3.12.1.43. Deve possuir mecanismo de classificação dinâmica do conteúdo do site, de acordo com o que está sendo carregado, a ferramenta deve atribuir uma categoria automática ao conteúdo e aplicar a política configurada;
4.3.12.1.44. A solução deve permitir consolidar todos os logs em uma única console;
4.3.12.1.45. Deve permitir criar buscas nos logs utilizando parâmetros como período, ação, nome da regra,

nome do malware, dispositivo, domínio, dentre outros;
4.3.12.1.46. Baseado no resultado de uma consulta, a solução deve permitir que o administrar possa salvar a consulta como favorita ou como um relatório em PDF;
4.3.12.1.47. A solução deve permitir alterar o tipo de exibição das informações dos logs para, pelo menos, gráficos de pizza, gráficos de linhas, gráficos de barras e tabela;
4.3.12.1.48. Deve permitir a criação de relatórios sob demanda e agendados (diário, semanal, mensal e definindo o período manualmente). Os relatórios devem possuir filtros por localidade/gateway e usuários;
4.3.12.1.49. Deverá fornecer pelo menos os seguintes relatórios: Aplicações mais utilizadas, Categorias e sites mais acessados, Usuários com maior número de acessos, Políticas violadas, maiores infratores, principais ameaças filtradas, dentre outros;
4.3.12.1.50. A solução deve possuir mecanismo que permita auditar as ações dos administradores, registrando as principais ações executadas. Os logs de auditoria devem ser exportados para arquivo offline como CSV;
4.3.12.1.51. Deve permitir o backup das políticas em arquivo;
4.3.12.1.52. O agente de monitoramento do tráfego deve possuir opção de desabilitar a filtragem temporariamente através de uma chave definida pelo administrador;
4.3.12.1.53. Para que o agente seja desinstalado, a solução deve prover mecanismo de proteção para que isso esteja disponível mediante senha configurada;
4.3.12.1.54. A solução deve permitir que o administrador receba notificações que incluam, pelo menos, notificações de sistema (falhas de autenticação, erro nos gateways), segurança (conteúdo malicioso, botnets) e uso de Internet (violação de políticas de tráfego);
4.3.12.1.55. Os alertas devem ser configurados para serem enviados a escopos distintos de usuários/administradores;
4.3.12.1.56. O agente de monitoramento de acesso deve possuir compatibilidade com Windows e MacOS.
4.3.12.1.57. O proxy local da solução deve ser capaz de permitir que o cliente instale a plataforma abaixo:
4.3.12.1.58. Qualquer plataforma compatível com Redhat Enterprise 7.x ou CentOS 7.x
4.3.12.1.59. Baremetal;
4.3.12.1.60. Plataforma virtualizada (VMWare, HyperV, KVM);
4.3.12.1.61. O proxy local da solução deve ser totalmente controlado pelo cliente.
4.3.12.1.62. O administrador deve ser capaz de adicionar mais recursos no gateway local sem mais assinaturas ou licenças.
4.3.12.1.63. O administrador deve ser capaz de acessar o gateway local via SSH para gerenciamento de rede.
4.3.12.1.64. A solução deve ser capaz de suportar o protocolo/método abaixo para autenticação do usuário:
4.3.12.1.64.1. Microsoft AD (até AD 2016);
4.3.12.1.64.2. Microsoft Azure AD;
4.3.12.1.64.3. Okta;
4.3.12.1.64.4. Microsoft ADFS;
4.3.12.1.64.5. Microsoft AD.
4.3.12.1.65. A solução deve ser capaz de sincronizar as informações do usuário do diretório para configurações de política;
4.3.12.1.66. A solução deve ser capaz de suportar vários domínios ao fazer as autenticações do usuário.

4.3.13. Proteção avançada para emails

4.3.13.1. Características Gerais da Solução
4.3.13.1.1. Em caso de nuvem, a solução deverá atender, no mínimo, os níveis de serviço abaixo:

Disponibilidade do serviço	98% ou maior de uptime
Proteção contra Vírus	Nenhum e-mail com vírus
Efetividade no bloqueio de SPAM	99% ou maior
Ocorrência de Falsos-positivos	Não mais que 0,0004%
Latência máxima na entrega de mensagens	Não mais que um minuto

4.3.13.1.2. A solução deverá possuir Single Sign-On para acessar o console de administração;
4.3.13.1.3. A solução deverá permitir a criação de regras para entrada (inbound) e saída (outbound) de e-mails;
4.3.13.1.4. A solução deverá possuir console de gerenciamento web;
4.3.13.1.5. A solução deverá possuir console centralizada, incluindo:
4.3.13.1.5.1. Configurações de administração;
4.3.13.1.5.2. Objetos de política;
4.3.13.1.5.3. Objetos suspeitos;
4.3.13.1.5.4. Gerenciamento de usuário final;
4.3.13.1.5.5. Gerenciamento de diretório;

4.3.13.1.5.6. Informações sobre licenciamento;
4.3.13.1.5.7. Logs;
4.3.13.1.5.8. Relatórios.
4.3.13.1.6. A solução deverá possuir dashboards possibilitando no mínimo a visualização de ameaças, ransomwares, detalhes de autenticação baseada em domínio, sandbox, BEC, SPAM, principais violações, eventos de DLP, consumo de banda, proteção Time-of-Click;
4.3.13.1.7. A solução deverá possuir configurações de dashboard sendo possível selecionar:
4.3.13.1.7.1. Direção do tráfego: entrada e saída de emails (inbound/outbound);
4.3.13.1.7.2. Período: data, semana e mês.
4.3.13.1.8. A solução deverá possuir métodos de autenticação como: Correspondência de IP do remetente, SPF (Sender Policy Framework); DKIM (DomainKeys Identified Mail) e DMARC (Authentication Message Reporting, Reporting & Conformity) baseado em domínio para proteger contra falsificação de email;
4.3.13.1.9. A solução deverá ser capaz de permitir a filtragem baseada em reputação IP para no mínimo: Remetentes permitidos com base no endereço IP e país
4.3.13.1.10. Remetentes bloqueados com base no endereço IP e país;
4.3.13.1.11. A solução deverá ser capaz de permitir a filtragem de remetente e destinatários para no mínimo: Remetentes aprovados por endereço de e-mail ou domínio, Remetentes bloqueados por endereço de e-mail ou domínio e validar destinatário de entrada de e-mail;
4.3.13.1.12. A solução deverá possibilitar incluir X-Header no cabeçalho da mensagem para mensagens de email correspondentes a remetentes aprovados;
4.3.13.1.13. A lista de remetentes aprovados e remetentes bloqueados deverão exibir no mínimo as seguintes informações:
4.3.13.1.13.1. Remetente;
4.3.13.1.13.2. Domínio do destinatário;
4.3.13.1.13.3. Data.
4.3.13.1.14. A solução deverá possuir Correspondência de IP do remetente, possibilitando especificar um IP ou um intervalo de endereços IP em um domínio do remetente identificado pelo endereço do cabeçalho da mensagem para permitir mensagens de email apenas desses endereços;
4.3.13.1.15. A solução deverá detectar malwares, worms, e outras ameaças baseadas em assinatura e padrões;
4.3.13.1.16. A solução deverá ser capaz de detectar spam baseado em assinatura e padrões;
4.3.13.1.17. A solução deverá identificar e-mails marketing como redes sociais, fóruns e boletins de informações;
4.3.13.1.18. A solução deverá permitir criar exceções para e-mails marketing;
4.3.13.1.19. A configuração de spam deverá possuir no mínimo três níveis: baixo, meio e alto;
4.3.13.1.20. A solução deverá detectar ataques de comprometimento de email;
4.3.13.1.21. A solução deverá possuir detectar phishing e conteúdos suspeitos;
4.3.13.1.22. A solução deverá detectar mensagens de graymail;
4.3.13.1.23. A solução deverá varreduras JSE e VBE para identificar ameaças de macro;
4.3.13.1.24. A solução deverá detectar ameaças desconhecidas utilizando machine learning;
4.3.13.1.25. A solução deverá permitir visualizar relatório detalhado para cada detecção Machine Learning;
4.3.13.1.26. A solução deverá possuir engine própria para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados;
4.3.13.1.27. A solução deverá possuir Proteção anti-ransomware;
4.3.13.1.28. A solução deverá possuir análise de URL's no corpo do e-mail;
4.3.13.1.29. A solução deverá possuir o recurso para analisar as URLs no momento do clique do usuário e as bloquear se forem maliciosas;
4.3.13.1.30. A solução deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito;
4.3.13.1.31. A solução deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito;
4.3.13.1.32. A solução deverá possuir Proteção contra Comprometimento de E-mail;
4.3.13.1.33. Deverá permitir adicionar usuários de alto perfil, possibilitando exportar a lista em CSV;
4.3.13.1.34. Deverá possibilitar importar usuários de alto perfil através de arquivo CSV;
4.3.13.1.35. A solução deverá fornecer informações detalhadas bem como razões para mensagens de email detectadas como possíveis ataques analisados ou prováveis do Business Email Compromise (BEC);
4.3.13.1.36. A solução deverá possuir Proteção contra-ataques de Engenharia Social;
4.3.13.1.37. A solução deverá fornecer informações detalhadas bem como razões para mensagens de email detectadas como possíveis ataques de engenharia social;
4.3.13.1.38. A solução deverá ser capaz utilizar no mínimo os seguintes bancos de dados de reputação que:
4.3.13.1.38.1. Tenham uma lista de endereços IP de servidores de correio que são conhecidos por serem fontes de spam;
4.3.13.1.38.2. Tenham uma lista de endereços IP identificados como envolvidos em ransomware ativos, malware ou outras campanhas de ameaças por email;
4.3.13.1.38.3. Tenham uma lista de IPs atribuídos dinamicamente.
4.3.13.1.39. A solução deverá possibilitar configurar diferentes tipos de exceções de varredura em um email através de definições de condições e possibilitando executar as ações ou equivalentes de bypass, deleção do email

incluindo anexos e quarentenar quando:

4.3.13.1.39.1. O número de arquivos em um arquivo compactado excede 353;

4.3.13.1.39.2. A taxa de descompactação de um arquivo compactado excede 100;

4.3.13.1.39.3. O número de camadas de descompactação em um arquivo compactado excede 20;

4.3.13.1.39.4. O tamanho de um único arquivo descompactado excede 60 MB;

4.3.13.1.39.5. Um arquivo do Office contém mais de 353 subarquivos.

4.3.13.1.40. Deverá possibilitar incluir Tag;

4.3.13.1.41. A solução deverá possuir regras de varredura avançadas que permitam especificar as condições que a regra se aplica às mensagens verificadas pela solução;

4.3.13.1.42. Deverá possuir as seguintes condições:

4.3.13.1.42.1. Tamanho da mensagem;

4.3.13.1.42.2. Assunto;

4.3.13.1.42.3. Corpo do email;

4.3.13.1.42.4. Cabeçalho;

4.3.13.1.42.5. Conteúdo do anexo;

4.3.13.1.42.6. Nome e/ou Extensão:

4.3.13.1.42.6.1. .386, .ACM,.ASP,.AVP, .BAT,.CGI, .CHM,.CLA,.CLASS,.CMD, .CNV, .COM, .CS, .DLL, .DRV, .EXE, .HLP, .HTA, .HTM, .JS*, .LNK, .OCX, .OPO, .PHP, .PL. .SH, .SYS, .VBS, VBE, VXD, .WBS, .WIZ. WSH, .DOC, .DOCM, DOCX, .DOT, .DOTM, .DOTX, .DVB, .EML, .MD*, .PPA, .PPAM, .PPS, .PPSM, .PPSX, .PPT, .PPTM, .PPTX, XL,XLA, XLAM, .XLC, .XLK, XLL,.XLM, .XLR, .XLS, .XLSB, .XLSM, XLSX, .XLT, .XLTM, XLTX;

4.3.13.1.42.7. MIME content-type: video, audio, imagens, documentos e outros;

4.3.13.1.42.8. Tamanho do anexo;

4.3.13.1.42.9. Anexo protegido por senha: .7z, .ace, .arj, .docx, .pptx, .rar, .xlsx, .zip;

4.3.13.1.42.10. Quantidade de anexos;

4.3.13.1.42.11. Número de destinatários.

4.3.13.1.43. A solução deverá as ações da regra permitindo definir o que acontecerá com as mensagens que atendem às condições dos critérios da regra:

4.3.13.1.43.1. Criptografar mensagem de email;

4.3.13.1.43.2. Monitorar, permitindo os administradores o monitoramento das mensagens. As ações de monitoramento incluem o envio de uma mensagem de notificação para outras pessoas ou o envio de uma cópia oculta (Cco) da mensagem para outras pessoas;

4.3.13.1.43.3. Bloqueio, deverá interceptar a mensagem, impedindo que ela atinja o destinatário original. As ações de bloqueio incluem excluir a mensagem inteira, colocar em quarentena e enviar para um destinatário diferente;

4.3.13.1.43.4. Modificar, permitindo alterar a mensagem e/ou seus anexos. As ações de modificação incluem limpeza de vírus que podem ser limpos, exclusão de anexos de mensagens, inserção de um carimbo no corpo da mensagem ou TAG de assunto.

4.3.13.1.44. A solução deverá possibilitar selecionar de Todas as correspondências ou equivalente para acionar a regra somente quando todos os critérios configurados selecionados fizerem correspondência;

4.3.13.1.45. A solução deverá possibilitar selecionar de quaisquer correspondências ou equivalente para acionar a regra quando qualquer critério configurado fizer correspondência;

4.3.13.1.46. Deve ser possível criar políticas de malwares, spam e filtragem de conteúdo com:

4.3.13.1.46.1. Definição do destinatário, possibilitando selecionar domínios cadastrados, domínios específicos e grupos de usuários;

4.3.13.1.46.2. Especificação de endereços de remetente;

4.3.13.1.46.3. Exceções.

4.3.13.1.47. A solução deverá possibilitar importar e exportar os destinatários, remetentes e listas de exceções;

4.3.13.1.48. Deve ser possível criar políticas que executem ações em mensagens que contêm malware, worms ou outros códigos maliciosos;

4.3.13.1.49. Deve ser possível realizar a limpeza de malwares ou códigos maliciosos, onde o malware pode ser removido com segurança do conteúdo do arquivo infectado, resultando em uma cópia não infectada da mensagem ou anexo original;

4.3.13.1.50. A solução deverá possuir o serviço de banner para customização do portal com a logo;

4.3.13.1.51. A solução deverá possuir integração com o Active Directory;

4.3.13.1.52. A solução deverá permitir o gerenciamento de múltiplos domínios;

4.3.13.1.53. A solução deverá permitir a integração com Microsoft Office 365, Google G-Suite e outros servidores de e-mail;

4.3.13.1.54. O uso das REST API's deve perimitir executar operações para no mínimo: criação, leitura, atualização e exclusão.

4.3.13.2. Criptografia de E-mail

4.3.13.2.1. A solução deverá ser capaz de criptografar e-mails baseado em políticas;

4.3.13.2.2. A solução deverá assegurar a comunicação através da utilização do protocolo TLS;

4.3.13.2.3. A solução deverá permitir a configuração da checagem do TLS;

4.3.13.2.4. A solução deverá suportar: TLS 1.2, TLS 1.1 and TLS 1.0.

4.3.13.3. Rastreamento de e-mail e Auditoria

4.3.13.3.1. A solução deve permitir o rastreamento de mensagens de forma centralizada e por meio da interface de gerenciamento, não sendo aceito pesquisa via linha de comando;

4.3.13.3.2. A solução deverá possuir permitir o rastreamento de mensagens enviadas e recebidas;

4.3.13.3.3. A solução deverá possibilitar pesquisas de log de rastreamento de email por até 30 dias;

4.3.13.3.4. A solução deverá fornecer buscas para rastreamento de email por: período, direção do tráfego, remetente, destinatário, tipo (bloqueado/liberado), ação, assunto, ID da mensagem e Hash do anexo SHA256;

4.3.13.3.5. Deverá possibilitar exportar a busca no formato .CSV;

4.3.13.3.6. A solução deverá possuir permitir a consulta de eventos com os logs das políticas aplicadas por até 30 dias;

4.3.13.3.7. A solução deverá fornecer consulta de eventos com os logs das políticas por: período, direção do tráfego, remetente, destinatário, nome da regra, tipo de ameaça, anexo, BEC, conteúdo, DLP, Graymail, ransomware,pishing,spam, malware, web reputation, ID da mensagem e ação;

4.3.13.3.8. A solução deverá permitir rastrear os cliques de URL por até 30 dias;

4.3.13.3.9. A solução deverá fornecer permitir rastrear os cliques de URL por: data,direção do tráfego, remetente, destinatário,ID da mensagem, URL, ação e a hora em que um URL foi clicada;

4.3.13.3.10. A solução deverá ser possível consultar os logs de auditoria da console da solução por até 30 dias;

4.3.13.3.11. Deverá ser possível encaminhar os logs para syslog.

4.3.13.4. Relatórios

4.3.13.4.1. A soluçaõ deverá fornecer relatórios com base em uma programação diária, semanal, mensal e trimestral;

4.3.13.4.2. Os relatórios deverão ser, pelo menos, no formato PDF;

4.3.13.4.3. Deverá ser possível criar relatório agendados e manuais;

4.3.13.4.4. Deverá ser possível obter relatório sobre com resumo do tráfego de email de todos os domínios e por domínio, detecções de ameaças, detecções de arquivos da sandbox, detecções de URL da sandbox e os principais destinatários comprometidos por email (BEC).

4.3.13.5. Notificações

4.3.13.5.1. A solução deverá suportar via notificação via e-mail;

4.3.13.5.2. A solução deverá possuir modelos de notificação pré-definidas para violação de políticas;

4.3.13.5.3. A solução deverá suportar notificar quando o e-mail possuir um anexo compactado;

4.3.13.5.4. A solução deverá notificar quando o e-mail quando o tamanho da mensagem excedido;

4.3.13.5.5. A solução deverá notificar quando uma regra for desencadeada;

4.3.13.5.6. A solução deverá notificar quando houver uma configuração de violação de segurança;

4.3.13.5.7. A solução deverá notificar quando um vírus e spam.

4.3.13.6. Prevenção contra Vazamento de Dados

4.3.13.6.1. A solução deverá permitir gerenciar as mensagens de email com dados confidenciais e proteger contra perda de dados, monitorando as mensagens de email de saída;

4.3.13.6.2. A solução deverá possibilitar criar regras por expressões regulares, palavras chaves e atributos do arquivo;

4.3.13.6.3. A solução deverá possuir templates pré-definidos;

4.3.13.6.4. A solução deverá possuir templates customizados;

4.3.13.6.5. A solução deverá possuir uma base com no mínimo 200 modelos para criação de regras;

4.3.13.6.6. A solução deverá permitir a customização de modelos aderência a LGPD.

4.3.13.7. Da quarentena

4.3.13.7.1. A solução deverá permitir visualizar as mensagens quarentenadas por data, direção do tráfego, remetente, destinatários e conteúdo;

4.3.13.7.2. A solução deverá permitir o gerenciamento da quarentena para múltiplos domínios;

4.3.13.7.3. A solução deverá permitir a customização da notificação de quarentena pela menos semanal, uma vez ou mais vezes durante o dia;

4.3.13.7.4. A notificação de quarentena deverá permitir a customização;

4.3.13.7.5. A notificação de quarentena deverá ser, no mínimo, em inglês e português;

4.3.13.7.6. A solução deverá possibilitar a gestão de quarentena de forma que seja possível que o administrador possa visualizar: a razão de um determinado bloqueio, o remetente, o destinatário, a data, o assunto, o IP do host de destino, a mensagem original, o tamanho da mensagem original;

4.3.13.7.7. Com base nos requisitos acima, deve ainda permitir as ações liberar e/ou excluir a mensagem;

4.3.13.7.8. A solução deverá permitir realizar o download da mensagem quarentenada

4.3.13.7.9. Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais as regras foram ativadas;

4.3.13.7.10. Deverá possuir single sign-on (SSO) para a quarentena de usuário;

4.3.13.7.11. Deverá possibilitar utilizar duplo fator de autenticação;

4.3.13.7.12. Deverá possibilitar que usuário tome as seguintes ações ou similar em sua própria quarentena:

4.3.13.7.12.1. Excluir e bloquear o remetente: possibilitando excluir permanentemente a mensagem e adicionar o endereço aos remetentes bloqueados;

4.3.13.7.12.2. Excluir, possibilitando excluir permanentemente a mensagem;
4.3.13.7.12.3. Entregar e aprovar o remetente, permitindo liberar a mensagem da quarentena e adicionar o endereço aos remetentes aprovados, para que mensagens futuras de remetentes aprovados não sejam mantidas em quarentena;
4.3.13.7.12.4. Entregar, permitindo assim liberar a mensagem da quarentena.
4.3.13.7.13. Deverá possibilitar que o usuário criar listas remetentes aprovados e remetentes bloqueados.

4.3.14. Módulo de proteção para ferramentas de e-mail e colaboração em nuvem (Office365)

4.3.14.1. A solução deve permitir a identificação e proteção contra ameaças no Microsoft Office 365 (Exchange Online, Sharepoint Online, Onedrive for Business e Microsoft Teams) e GSuite;
4.3.14.2. Identificar e bloquear arquivos maliciosos carregados para o Google Drive, Onedrive, Sharepoint e Microsoft Teams. Por exemplo, se um usuário tentar carregar um determinado arquivo malicioso ou proibido em uma das plataformas citadas, a solução deve fazer o bloqueio;
4.3.14.3. Bloquear upload de arquivos por tipo definido em política para as soluções supracitadas;
4.3.14.4. Identificar e bloquear URLs maliciosas em arquivos e URLs, incluindo URLs dentro de anexos;
4.3.14.5. Realizar escaneamentos de ameaças em tempo-real nos serviços integrados, identificando componentes maliciosos;
4.3.14.6. Permitir realizar escaneamento retroativo de ameaças (sob demanda), isto é, em busca de ameaças já armazenadas nas caixas de email dos usuários ou em diretórios do Google Drive, Onedrive e Sharepoint;
4.3.14.7. O nível de sensibilidade das URLs maliciosas deve ser configurável através de políticas;
4.3.14.8. Deve possuir capacidade de cadastro dos usuários importantes para focar a análise de ataques de Comprometimento de Email (BEC);
4.3.14.9. Deve permitir que os administradores configurem a periodicidade das notificações para, no mínimo, URLs maliciosas identificadas, SPAMs maliciosos, Phishing, Ransomware, arquivos analisados na sandbox e identificados como baixo, médio e alto risco;
4.3.14.10. Identificar tentativas de Comprometimento de Email baseado em uma análise dos estilos de escrita de cada usuário cadastrado como importante;
4.3.14.11. A solução deve permitir a visualização das estatísticas no dashboard por serviço integrado (Gmail, Google Drive, Exchange Online, Teams, Onedrive, Sharepoint) e alterar o período dos logs para, no mínimo, 24 horas, 7 dias e 30 dias;
4.3.14.12. Deve permitir a exibição da tendência para cada um dos tipos de serviço integrado em relação ao mesmo período anterior. Por exemplo, exibir aumento ou redução das ameaças no Exchange Online nos últimos 30 dias, comparando com os 30 dias anteriores;
4.3.14.13. Deve ter a capacidade de analisar arquivos e URLs em sandbox para identificação de ameaças desconhecidas (sem assinatura);
4.3.14.14. Deve utilizar mecanismos de proteção que contemplem, pelo menos, malwares conhecidos por assinatura, malwares desconhecidos por Machine Learning, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URLs;
4.3.14.15. A solução deve permitir compartilhamento de informações através de SIEM via API ou através da gerência centralizada;
4.3.14.16. A solução deve prover relatórios que contemplem, pelo menos, riscos de segurança (ameaças), ransomware, arquivos analisados em sandbox, auditoria e sobre a API;
4.3.14.17. Os relatórios devem ser exportáveis para, pelo menos, PDF;
4.3.14.18. Os relatórios devem ser enviados por email, mediante configuração do administrador;
4.3.14.19. A solução ofertada deve contemplar uma plataforma de simulação de phishing e conscientização de usuários sem necessidade de licenciamento adicional;
4.3.14.20. A verificação Anti-malware deverá permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.
4.3.14.21. Realizar integração nuvem-a-nuvem, através de API da Microsoft e Google;
4.3.14.22. As ações configuráveis nas políticas do serviço de email devem contemplar, no mínimo, etiquetar a mensagem (inserir tag), quarentenar, deletar, ignorar e mover para lixeira;
4.3.14.23. Os demais serviços devem possuir ações pré-definidas e configuráveis para eliminar, quarentenar e ignorar os arquivos identificados;
4.3.14.24. Deve empregar o uso de análise em ambiente virtual (sandbox) do próprio fabricante para detecção de malwares avançados, com objetivo de diminuir seu risco de violação;
4.3.14.25. As políticas deverão ser aplicáveis por usuário ou grupo sincronizado da estrutura de serviço online (Microsoft ou Google);
4.3.14.26. Possuir um dashboard com as principais ameaças detectadas, a exemplo dos tipos Ransomware, Phishing, Comprometimento de E-mail.
4.3.14.27. A solução deverá ser capaz de implementar políticas com base no filtro de conteúdo das mensagens;
4.3.14.28. A solução deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em sandbox com a gerência centralizada do fabricante;
4.3.14.29. Cada política de serviço deve ser configurável para apenas monitorar ou tomar ação de proteção;
4.3.14.30. As notificações enviadas para o administrador e para os usuários devem ser customizáveis, permitindo tradução, inclusão ou exclusão de campos;
4.3.14.31. Deverá permitir a configuração dos níveis de detecção para SPAM;

4.3.14.32. Deverá permitir o administrador criar exceções para permitir ou bloquear determinados endereços de email e URLs manualmente;
4.3.14.33. A solução deve possuir capacidade de ignorar emails já enviados para a lixeira do serviço de email;
4.3.14.34. Deve permitir ao administrador bloquear mensagens de graymail por tipo (mensagens de marketing, notificações de fóruns e redes sociais, etc);
4.3.14.35. Os logs devem ser interativos, permitindo ao administrador montar consultas baseadas nos parâmetros como serviço detectado, tipo/categoria da ameaça, usuários afetados, política acionada, nome da ameaça, dentre outros;
4.3.14.36. Os resultados das consultas de logs deverão ter opção de salvar como um relatório exportável;
4.3.14.37. A solução deve permitir que o administrador realize buscas pontuais nos logs, a partir de parâmetros previamente definidos;
4.3.14.38. Deve possuir áreas de quarentena distintas para cada um dos serviços integrados, permitindo a restauração, download ou exclusão de arquivos/emails quarentenados pela política;
4.3.14.39. Deve permitir a criação de exceções para detecções por Machine Learning e por Sandbox;
4.3.14.40. A solução deve ter a capacidade de integração com serviços de autenticação para logon único (single sign-on) com, pelo menos, Okta, ADFS e Azure AD.
4.3.14.41. Deve possuir capacidade de configuração de contas de administração com permissões granulares por administrador, permitindo visualização ou controle total dos itens de menu;
4.3.14.42. Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação;
4.3.14.43. Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.
4.3.14.44. O recurso de detecção e resposta para e-mails deverá ser integrado à solução da Microsoft Office 365 sem a necessidade de alterar configurações dos serviços de e-mail, ou configurações dos usuários;
4.3.14.45. Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente;
4.3.14.46. A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;
4.3.14.47. Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam;
4.3.14.48. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
4.3.14.49. Em caso de ameaça avançada por email, a solução deve permitir tomar diferentes ações de resposta no ambiente, contemplando, no mínimo:
4.3.14.49.1. Permitir adicionar o remetente (sender) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários internos;
4.3.14.49.2. Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas;
4.3.14.49.3. Deletar o e-mail selecionado das caixas selecionadas.

4.4. SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 MESES

4.4.1. Características Gerais Da Solução
4.4.1.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:
4.4.1.1.1. Windows Server 2000;
4.4.1.1.2. Windows Server 2003 SP1 e 2003 R2 SP2;
4.4.1.1.3. Windows Server 2008 e 2008 R2;
4.4.1.1.4. Windows Server 2012 e 2012 R2;
4.4.1.1.5. Windows Server 2016;
4.4.1.1.6. Windows Server 2019;
4.4.1.1.7. Windows Server 2022;
4.4.1.1.8. Red Hat Enterprise 5, 6, 7 e 8;
4.4.1.1.9. CentOS 5, 6, 7 e 8;
4.4.1.1.10. AIX 6.1, 7.1 e 7.2;
4.4.1.1.11. Oracle Linux 5, 6, 7 e 8;
4.4.1.1.12. SUSE Linux Enterprise Server 10, 11, 12 e 15;
4.4.1.1.13. Ubuntu 10, 12, 14, 16, 18 e 20;
4.4.1.1.14. Debian 6, 7, 8, 9 e 10;
4.4.1.1.15. Rocky Linux 8;
4.4.1.1.16. AlmaLinux 8;
4.4.1.1.17. Cloud Linux 5, 6, 7 e 8;
4.4.1.1.18. Solaris 10 1/13 Sparc;
4.4.1.1.19. Solaris 10 1/13 (x86/x64);
4.4.1.1.20. Solaris 11.2/ 11.3 Sparc;
4.4.1.1.21. Solaris 11.2/ 11.3 (x86/x64);
4.4.1.1.22. Solaris 11.4 (x86, x64 ou SPARC)

4.4.1.1.23. Amazon Linux e Amazon Linux 2 (x64).
4.4.1.2. A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;
4.4.1.3. A console de gerenciamento deverá ser em nuvem ou on-premises, permitindo o gerenciamento das políticas de segurança através da Internet;
4.4.1.4. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;
4.4.1.5. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;
4.4.1.6. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
4.4.1.7. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;
4.4.1.8. A console de administração deverá permitir o envio de notificações via SMTP;
4.4.1.9. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
4.4.1.10. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
4.4.1.11. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;
4.4.1.12. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
4.4.1.13. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;
4.4.1.14. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;
4.4.1.15. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
4.4.1.16. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;
4.4.1.17. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;
4.4.1.18. A solução de segurança ter a capacidade de identificar ataques entre conteineres;
4.4.1.19. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
4.4.1.20. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar políticas de segurança;
4.4.1.21. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
4.4.1.22. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
4.4.1.23. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
4.4.1.24. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;
4.4.1.25. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;
4.4.1.26. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;
4.4.1.27. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;
4.4.1.28. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;
4.4.1.29. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;
4.4.1.30. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;
4.4.1.31. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
4.4.1.32. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
4.4.1.33. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;
4.4.1.34. A solução deverá mostrar quais máquinas estão usando determinada política;
4.4.1.35. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
4.4.1.36. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

4.4.1.37. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;
4.4.1.38. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
4.4.1.39. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
4.4.1.40. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
4.4.1.41. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
4.4.1.42. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
4.4.1.43. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArcSight de modo a permitir enviar os seus logs para essas soluções;
4.4.1.44. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
4.4.1.45. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
4.4.1.46. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
4.4.1.47. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
4.4.1.48. Após a atualização deve ser informado o que foi modificado ou adicionado;
4.4.1.49. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;
4.4.1.50. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;
4.4.1.51. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
4.4.1.52. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
4.4.1.53. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;
4.4.1.54. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
4.4.1.55. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;
4.4.1.56. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
4.4.1.57. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
4.4.1.58. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
4.4.1.59. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;
4.4.1.60. A solução deve possuir API documentada para integração na esteira de automação;
4.4.1.61. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;
4.4.1.62. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
4.4.1.63. A solução deve permitir desabilitar os módulos individualmente;
4.4.1.64. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.

4.4.2. Antimalware
4.4.2.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
4.4.2.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
4.4.2.3. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;
4.4.2.4. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;
4.4.2.5. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do

arquivo;
4.4.2.6. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;
4.4.2.7. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;
4.4.2.8. A solução deverá oferecer escanear processos em memória em busca de Malware;
4.4.2.9. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;
4.4.2.10. O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;
4.4.2.11. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;
4.4.2.12. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;
4.4.2.13. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);
4.4.2.14. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;
4.4.2.15. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;
4.4.2.16. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;
4.4.2.17. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;
4.4.2.18. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;
4.4.2.19. Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;
4.4.2.20. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

4.4.3. Proteção Contra URLs Maliciosas
4.4.3.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;
4.4.3.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
4.4.3.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;
4.4.3.4. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;
4.4.3.5. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;
4.4.3.6. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;
4.4.3.7. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;
4.4.3.8. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

4.4.4. Firewall
4.4.4.1. Operar como firewall de host, através da instalação de agente nos servidores protegidos;
4.4.4.2. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;
4.4.4.3. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;
4.4.4.4. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;
4.4.4.5. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;
4.4.4.6. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;
4.4.4.7. Precisa ter a capacidade de definição de regras para contextos específicos;
4.4.4.8. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;
4.4.4.9. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
4.4.4.10. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
4.4.4.11. O firewall deverá ser stateful bidirecional;
4.4.4.12. O firewall deverá permitir liberar ou apenas logar eventos;
4.4.4.13. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;
4.4.4.14. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;
4.4.4.15. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;
4.4.4.16. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

4.4.4.17. Deverá realizar pseudo stateful em tráfego UDP;
4.4.4.18. Deverá logar a atividade stateful;
4.4.4.19. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;
4.4.4.20. Deverá permitir limitar o número de meias conexões vindas de um computador;
4.4.4.21. Deverá prevenir ack storm;
4.4.4.22. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;
4.4.4.23. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período configurado pelo administrador;
4.4.4.24. Deverá permitir criar lista de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede;
4.4.4.25. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

4.4.5. Proteção De Vulnerabilidades De S.O. E Aplicações

4.4.5.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
4.4.5.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
4.4.5.3. A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;
4.4.5.4. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;
4.4.5.5. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;
4.4.5.6. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
4.4.5.7. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
4.4.5.8. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;
4.4.5.9. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
4.4.5.10. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
4.4.5.11. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;
4.4.5.12. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
4.4.5.13. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
4.4.5.14. Deverá ser capaz de inspecionar tráfego criptografado de entrada;
4.4.5.15. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;
4.4.5.16. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
4.4.5.17. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
4.4.5.18. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
4.4.5.19. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
4.4.5.20. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
4.4.5.21. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
4.4.5.22. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
4.4.5.23. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;
4.4.5.24. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

4.4.5.25. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;
4.4.5.26. As regras devem ser atualizadas automaticamente pelo fabricante;
4.4.5.27. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

4.4.6. Monitoramento De Integridade
4.4.6.1. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;
4.4.6.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
4.4.6.3. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;
4.4.6.4. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;
4.4.6.5. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
4.4.6.6. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;
4.4.6.7. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
4.4.6.8. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;
4.4.6.9. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real- time para ambiente Linux;
4.4.6.10. Deverá logar e colocar em relatório todas as modificações que ocorram;
4.4.6.11. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
4.4.6.12. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
4.4.6.13. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
4.4.6.14. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

4.4.7. Inspeção De Logs
4.4.7.1. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;
4.4.7.2. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
4.4.7.3. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
4.4.7.4. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
4.4.7.5. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
4.4.7.6. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;
4.4.7.7. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;
4.4.7.8. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;
4.4.7.9. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;
4.4.7.10. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;
4.4.7.11. As regras poderão ser modificadas por severidade de ocorrência de eventos;
4.4.7.12. As regras devem se atualizar automaticamente pelo fabricante;
4.4.7.13. Permitir modificação pelo administrador em regras para adequação ao ambiente.

4.4.8. Controle De Aplicações
4.4.8.1. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;
4.4.8.2. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
4.4.8.3. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;
4.4.8.4. A console deverá exibir eventos de no mínimo 30 dias;
4.4.8.5. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;
4.4.8.6. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

4.4.9. Detecção e Resposta

4.4.9.1. A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;
4.4.9.2. A solução deve possuir módulo de investigação, detecção integrados;
4.4.9.3. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
4.4.9.4. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;
4.4.9.5. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
4.4.9.6. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;
4.4.9.7. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
4.4.9.8. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
4.4.9.9. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;
4.4.9.10. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
4.4.9.11. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
4.4.9.12. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
4.4.9.13. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
4.4.9.14. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;
4.4.9.15. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
4.4.9.16. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
4.4.9.17. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
4.4.9.18. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

4.5. SOLUÇÃO DE SEGURANÇA CONTRA AMEAÇAS AVANÇADAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 MESES

4.5.1. A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;
4.5.2. Deve ser dimensionada para inspecionar 04Gbps de throughput;
4.5.3. A solução ofertada deve ser do mesmo fabricante da solução de software tendo como características mínimas:
4.5.3.1. Porta de gerenciamento 10/100/1000 base-T RJ45 port x 1 e iDrac enterprise RJ45 x 1
4.5.3.2. Porta de dados 10 Gb SFP+ SR transceiver x 4 10/100/1000 base-T RJ45 port x 5
4.5.3.3. Power supply 750W redundante
4.5.4. Funcionalidades e Requisitos específicos:
4.5.4.1. Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos:
4.5.4.1.1. Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;
4.5.4.1.2. Detecção de ataques direcionados;
4.5.4.1.3. Analisador virtual de ameaças;
4.5.4.1.4. Correlação de regras para detecção de conteúdo malicioso;
4.5.4.1.5. Análise de todos os estágios de uma sequência de ataques.
4.5.5. Esta solução deverá ser atendida através do fornecimento de solução de um único Fabricante, contendo:
4.5.5.1. Serviço de Monitoração e Análise de Ameaças Digitais em rede;
4.5.5.2. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;
4.5.5.3. Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network Exploit, web Exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;
4.5.5.4. Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;
4.5.5.5. Análise e correlação de atividades maliciosas tais como: Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede; Detecção de vermes de rede e de e-mail no tráfego de rede; Detecção de programas de exploração de vulnerabilidades (Exploits) na rede; Detecção de empacotamentos maliciosos no tráfego da rede;
4.5.5.6. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;
4.5.5.7. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.

4.5.6. Permitir a rápida identificação da criticidade dos eventos de segurança
4.5.7. Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;
4.5.8. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;
4.5.9. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;
4.5.10. Permitir a integração com sistemas de serviço de diretório;
4.5.11. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;
4.5.12. A análise de SMTP poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos;
4.5.13. A capacidade de análise de artefatos em sandbox pode ser realizada através de integração com serviço em nuvem do próprio fabricante;
4.5.14. A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;
4.5.15. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;
4.5.16. Deve possuir pelo menos 1 sensor para inspecionar o tráfego de rede de throughput de 04Gbps de análise;
4.5.17. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;
4.5.18. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;
4.5.19. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;
4.5.20. Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;
4.5.21. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;
4.5.22. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;
4.5.23. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;
4.5.24. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;
4.5.25. Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;
4.5.26. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;
4.5.27. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;
4.5.28. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;
4.5.29. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;
4.5.30. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;
4.5.31. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);
4.5.32. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;
4.5.33. Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);
4.5.34. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;
4.5.35. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches;
4.5.36. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;
4.5.37. Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;
4.5.38. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;
4.5.39. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;
4.5.40. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;
4.5.41. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;
4.5.42. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

4.5.43. Deve possuir interface web para busca e investigação local de incidentes;
4.5.44. Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Windows 7 SP1 e Windows 10;
4.5.45. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;
4.5.46. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;
4.5.47. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;
4.5.48. Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;
4.5.49. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:
- 4.5.49.1. Resumidos;
- 4.5.49.2. Visão Geral dos Incidentes de Segurança
- 4.5.49.3. Discriminação dos Tipos de Incidentes
- 4.5.49.4. Top Ameaças Analisadas
- 4.5.49.5. Top Hosts Infectados
- 4.5.49.6. Recomendações de Segurança
- 4.5.49.7. Executivos;
- 4.5.49.8. Deve possuir detalhes técnicos dos incidentes detectados;
- 4.5.49.9. Deve possuir estatística do tráfego analisado;
- 4.5.49.10. Deve possuir indicadores de risco do ambiente;
- 4.5.49.11. Recomendações de Segurança.

4.5.50. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;
4.5.51. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas etc.;
4.5.52. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;
4.5.53. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;
4.5.54. Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);
4.5.55. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;
4.5.56. Deve ser capaz de detectar tentativas de scan de rede;
4.5.57. Deve ser capaz de detectar propagação de malwares na rede;
4.5.58. Deve ser capaz de detectar tentativas de brute-force;
4.5.59. Deve ser capaz de detectar tentativas de fuga e roubo de informação;
4.5.60. Deve ser capaz de detectar ameaças que se replicam na rede;
4.5.61. Deve ser capaz de detectar Exploits na rede;
4.5.62. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);
4.5.63. A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;
4.5.64. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;
4.5.65. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;
4.5.66. Capacidade de salvar uma investigação antes de ser finalizada;
4.5.67. Capacidade de restaurar uma investigação para continuá-la ou consultá-la;
4.5.68. Capacidade de emitir relatórios baseados nas investigações;
4.5.69. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;
4.5.70. Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;
4.5.71. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;
4.5.72. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);
4.5.73. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;
4.5.74. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;
4.5.75. Deve permitir recebimento de logs via syslog;
4.5.76. Deve permitir encaminhamento de logs via syslog;
4.5.77. Deve permitir receber logs de diferentes dispositivos;
4.5.78. Deve possuir engine de correlação de eventos;
4.5.79. Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;
4.5.80. Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes;
4.5.81. Deve permitir a configuração de alarmes personalizados, com base em investigações;
4.5.82. Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;

4.5.83. A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;
4.5.84. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e análise;
4.5.85. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;
4.5.86. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;
4.5.87. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;
4.5.88. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;
4.5.89. A console de gerenciamento deverá ser gerenciada por Internet Explorer, Google Chrome e Firefox;
4.5.90. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;
4.5.91. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;
4.5.92. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;
4.5.93. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:
4.5.93.1. Uso de CPU
4.5.93.2. Uso de Disco;
4.5.93.3. Uso de Memória;
4.5.93.4. Tráfego malicioso analisado;
4.5.93.5. Todo o tráfego analisado.
4.5.94. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:
4.5.94.1. Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;
4.5.94.2. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.
4.5.95. A solução deverá ter integração com ferramentas de SIEM;
4.5.96. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;
4.5.97. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor;
4.5.98. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:
4.5.98.1. Computadores infectados;
4.5.98.2. Origem de infecções;
4.5.98.3. Estatísticas de ameaças;
4.5.98.4. Riscos potenciais de segurança;
4.5.98.5. Riscos de perda de informações;
4.5.98.6. Risco de sistema comprometido;
4.5.98.7. Risco de disseminação de ameaças;
4.5.98.8. Eventos suspeitos;
4.5.98.9. Infecções de malware.
4.5.99. A solução deverá apresentar função de pesquisa por logs contendo no mínimo:
4.5.99.1.1. Critérios de pesquisa por dia, mês e ano.
4.5.99.2. Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;
4.5.99.3. Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;
4.5.99.4. Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.
4.5.100. Módulo de Detecção e Resposta
4.5.100.1. A solução deve ter a capacidade de integrar-se com a plataforma de investigação e resposta centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;
4.5.100.2. A funcionalidade deve ser licenciada para analisar o throughput total do appliance;
4.5.100.3. A solução deve permitir a integração dos eventos ocorridos em outros segmentos de rede e outros appliances com objetivo de correlacionar os ataques na rede;
4.5.100.4. Deve permitir a análise em linha de tempo gráfica, representando a sequência da comunicação dos ativos, bem como seu protocolo e direção;
4.5.100.5. Deve identificar tentativas de ataques avançados na rede da CONTRATANTE e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;
4.5.100.6. Caso necessário, a CONTRATANTE pode optar em direcionar parte do licenciamento deste módulo para

outros módulos da plataforma de Detecção e Resposta, como o monitoramento do email, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento;

4.5.100.7. Ao clicar em um dos objetos identificados pela solução de inspeção de rede, a plataforma deverá informar um resumo do ataque em questão, contendo o IP/hostname envolvido, quais protocolos, atividades maliciosas, severidade do incidente, fases do ataque;

4.5.100.8. Deve exibir de forma e em tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs).

4.5.101. Características para o sensor de cargas de trabalho (aplicável ao item 04)

4.5.101.1. A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

4.5.101.2. A solução deve possuir módulo de investigação, detecção integrados;

4.5.101.3. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

4.5.101.4. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

4.5.101.5. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

4.5.101.6. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

4.5.101.7. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

4.5.101.8. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

4.5.101.9. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

4.5.101.10. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

4.5.101.11. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

4.5.101.12. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

4.5.101.13. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

4.5.101.14. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

4.5.101.15. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

4.5.101.16. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

4.5.101.17. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

4.5.101.18. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

4.6. SOLUÇÃO DE PROTEÇÃO PARA SERVIÇOS EM NUVEM COM VALIDAÇÃO DE MELHORES PRÁTICAS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES

4.6.1. Características gerais

4.6.1.1. A solução deve funcionar no sistema de análise de metadados via API, sem acesso de leitura ou gravação de dados;

4.6.1.2. Deve permitir gerenciar múltiplas contas de múltiplos serviços de nuvem a partir da mesma console;

4.6.1.3. Deve utilizar como base os pilares do AWS Well Architected Framework, exibindo ao menos, os pilares de Segurança, Confiabilidade, Eficiência de desempenho, Otimização de custos e Sustentabilidade;

4.6.1.4. Deverá integrar com, pelo menos, as seguintes ferramentas: ServiceNow, JIRA, PagerDuty, Microsoft Teams e Slack;

4.6.1.5. O fabricante deve possuir uma base de conhecimento com um catálogo de regras e controles de infraestrutura;

4.6.1.6. As regras na base de conhecimento devem contemplar, pelo menos, AWS e Microsoft Azure;

4.6.1.7. Deve possuir regras de correção/remediação;

4.6.1.8. Deve permitir a verificação da conformidade com padrões de mercado, dando visibilidade de, ao menos, LGPD, SOC2, NIST, CIS, PCI-DSS, GDPR e HIPAA;

4.6.1.9. Deve monitorar atividades e alterações das configurações das contas em tempo real;

4.6.1.10. Deve suportar a geração e exportação de relatórios baseados nos padrões de conformidade;

4.6.1.11. A solução deve suportar criação de regras personalizadas;

4.6.1.12. O dashboard deve exibir um resumo das contas integradas à console, informando o percentual de conformidade das contas;

4.6.1.13. A solução deverá informar quantas verificações foram realizadas e qual o resultado, se o controle está em conformidade ou falhou;

4.6.1.14. Ao clicar para visualizar todas as regras, deve ser possível visualizá-las por regra, por recurso (serviço) e por framework/padrão;

4.6.1.15. Deve ser possível filtrar as regras ao menos por: serviço, tipo do recurso, categorias, frameworks/padrões, regiões do serviço, regras, nível de risco, status, por data das verificações;

4.6.1.16. Usuários com permissão administrativa devem ter a possibilidade de suprimir ou ocultar regras identificadas;
4.6.1.17. Os achados dos scans devem estar disponíveis na console, exibindo o nível de risco da inconformidade, tendo pelo menos, os níveis baixos, médio, alto e muito alto;
4.6.1.18. O dashboard deve exibir o nível de conformidade por conta, informando esse nível por categorias, tendo ao menos, conformidade geral da conta, segurança, otimização de custos, excelência operacional, confiabilidade, sustentabilidade e eficiência de desempenho;
4.6.1.19. A console deve exibir um resumo das últimas atividades realizadas pelos usuários e os últimos eventos detectados. Para ambos, deve haver um link ou botão para visualizar os logs completos;
4.6.1.20. Para cada um dos níveis de conformidade exibidos, a solução deve disponibilizar um botão ou link para o detalhamento das detecções;
4.6.1.21. A solução deve exibir um histórico de 30 dias do nível de conformidade da conta, por categoria;
4.6.1.22. A console deve informar quais são as falhas mais críticas, bem como um link para a base de conhecimento que deverá explicar como corrigir a falha;
4.6.1.23. Deve ser possível filtrar os dados do dashboard por conta integrada, exibindo as informações pertinentes a todas as contas ou a uma conta selecionada;
4.6.1.24. Através da console, deve ser possível escanear templates antes de colocá-lo em produção;
4.6.1.25. A solução deve permitir o envio de notificações por email e por telefone;
4.6.1.26. Deve suportar autenticação multifator para cada usuário cadastrado;
4.6.1.27. Deve ser possível criar chaves de API através da console.

4.7. SOLUÇÃO DE PROTEÇÃO PARA ÁREAS DE ARMAZENAMENTO DE ARQUIVOS EM NUVEM, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES

4.7.1. Características gerais
4.7.1.1. A solução deve ter a capacidade de escanear arquivos em áreas de armazenamento em nuvem (cloud storage);
4.7.1.2. Deverá identificar malwares, incluindo virus, cavalos de troia, spyware e outros;
4.7.1.3. Deve escanear os arquivos independentes do seu tipo e tamanho;
4.7.1.4. A média de tempo de escaneamento deve ser inferior a 30 segundos para os arquivos;
4.7.1.5. A solução deve ser escalável e executar múltiplos escaneamentos simultaneamente;
4.7.1.6. O deploy da solução deverá ser realizado utilizando templates;
4.7.1.7. Deve suportar, pelo menos, o serviço Amazon Simple Storage Services (S3);
4.7.1.8. Deve identificar arquivos maliciosos através de:
4.7.1.8.1. Reputação, através da rede de ameaças do fabricante;
4.7.1.8.2. Proteção de variante para identificar malwares modificados por algoritmos polimórficos ou de obfuscação;
4.7.1.9. Permitir integrar com o fluxo de trabalho do cliente para identificar arquivos maliciosos no momento do upload;
4.7.1.10. Deve possuir arquitetura que permita criar buckets/áreas de quarentena para arquivos maliciosos identificados durante o scan;
4.7.1.11. Deve permitir a identificação dos arquivos através de tags para uso no fluxo de trabalho;
4.7.1.12. Deve suportar o escaneamento de, pelo menos, os seguintes tipos de arquivos: bin, exe, jpeg, mp4, pdf, txt e zip;
4.7.1.13. Deve possuir documentação de API pública no site do fabricante e acessível através da console de gerenciamento.

4.8. TREINAMENTO OFICIAL

4.8.1. Deverão ser fornecidos vouchers para treinamento oficial com especialista devidamente credenciado pelo fabricante;
4.8.2. Os vouchers devem permitir que a CONTRATANTE selecione os treinamentos e certificações no portfólio do fabricante de acordo com sua demanda de capacitação da equipe durante toda a vigência do contrato, respeitando a quantidade máxima de vouchers;
4.8.3. O treinamento poderá ser realizado de forma presencial ou remota, de acordo com as medidas sanitárias e legais vigentes durante o período de realização;
4.8.4. No caso de treinamento presencial, a CONTRATANTE deve arcar com as despesas de passagem, hospedagem e todos os custos relacionados a viagem.
4.8.5. O treinamento deverá ser apresentado no idioma português do Brasil;
4.8.6. Durante o treinamento, devem ser fornecidos os materiais necessários para que o participante possa consultar e estudar;
4.8.7. Os laboratórios e infraestruturas necessárias para realização do treinamento devem ser de responsabilidade da CONTRATADA, permitindo que os participantes apenas utilizem um computador para acessar o ambiente;
4.8.8. Ao final do treinamento, o voucher fornecido deverá permitir que o participante do treinamento realize uma prova de comprovação dos conhecimentos adquiridos e, caso seja aprovado, deverá receber a certificação de especialista por parte do fabricante;
4.8.9. A certificação fornecida ao fim do treinamento e aprovação deve ser válida por, pelo menos, 2 anos;

4.8.10. Caso o participante seja reprovado, o voucher deve permitir que ele refaça a prova após um período pré-definido sem custo adicional.

4.9. SERVIÇO DE SUPORTE ESPECIALIZADO PARA INSTALAÇÃO, MIGRAÇÃO E SUPORTE PREVENTIVO/CORRETIVO

4.9.1. Serviço de suporte especializado para ajustes, configurações, migrações e implementação da solução a ser fornecida;
4.9.2. Faz parte do escopo do serviço: Serviço inicial de instalação e configuração, suporte corretivo e preventivo especializado para funcionamento da solução, serviço de integração com as ferramentas suportadas pela solução e que façam parte do catálogo de ferramentas da CONTRATANTE, e quaisquer outros serviços que digam respeito a solução contratada;
4.9.3. Para prestação destes serviços, a CONTRATADA deverá empregar funcionários devidamente qualificados na utilização desse tipo de ferramenta, a ser comprovado através de apresentação de certificados emitidos pelo próprio fabricante, ou instituições por ele autorizados;
4.9.4. A CONTRATADA deverá prover equipe técnica especializada própria para atuar nas demandas da CONTRATANTE durante o contrato vigente.
4.9.5. O serviço em questão deve atuar em conjunto com o suporte especializado do fabricante para atuação na manutenção e aplicação das melhores práticas no ambiente;
4.9.6. DETALHAMENTO DO SERVIÇO DE INSTALAÇÃO E ATUALIZAÇÃO:
4.9.6.1. TRENDMICRO Smart Protection Complete, TRENDMICRO workload security; e TRENDMICRO Deep Discovery
4.9.6.1.1. Fase de Abertura:
4.9.6.1.1.1. Validar e Homologar escopo do projeto;
4.9.6.1.1.2. Validar objetivos e premissas do projeto;
4.9.6.1.1.3. Validar riscos e restrições do projeto;
4.9.6.1.1.4. Identificar e validar os requisitos do projeto.
4.9.6.1.2. Fase de Planejamento:
4.9.6.1.2.1. Elaborar plano de projeto;
4.9.6.1.2.2. Definir as pessoas envolvidas por parte do CONTRATANTE no projeto;
4.9.6.1.2.3. Reunir as equipes da CONTRATADA e CONTRATANTE;
4.9.6.1.2.4. Apresentação do cronograma do projeto com os prazos e responsabilidades;
4.9.6.1.2.5. Verificar os pré-requisitos do projeto;
4.9.6.1.2.6. Apresentar plano do projeto para a homologação por parte do CONTRATANTE.
4.9.6.1.3. Fase de Execução para Apex One:
4.9.6.1.3.1. Atualização do Apex One para a versão mais estável mais atualizada nova para 100 (cem) estações de trabalho e habilitação o XDR;
4.9.6.1.3.2. Passagem de conhecimento para a equipe da CONTRATANTE para que seja completada a migração nas demais estações de trabalho;
4.9.6.1.3.3. Redefinição da política de atualização automática;
4.9.6.1.4. Fase de Execução para Apex Central:
4.9.6.1.4.1. Atualização do Apex Central para a versão estável mais atualizada;
4.9.6.1.4.2. Treinamento Hands On.
4.9.6.1.5. Fase de Execução para Application Control:
4.9.6.1.5.1. Implantação do Application Control para a versão estável mais atualizada para 100 (cem) estações de trabalho;
4.9.6.1.5.2. Passagem de conhecimento para a equipe da CONTRATANTE para que seja completada a migração nas demais estações de trabalho;
4.9.6.1.6. Fase de Execução para Vulnerability Protection:
4.9.6.1.6.1. Realização de atualização da versão do Vulnerability Protection para a versão estável mais atualizada para 100 (cem) estações de trabalho;
4.9.6.1.6.2. Passagem de conhecimento para a equipe da CONTRATANTE para que seja completada a migração nas demais estações de trabalho;
4.9.6.1.6.3. Definição de política de proteção.
4.9.6.1.7. Fase de Execução para Workload Security e XDR integrado ao Vision One:
4.9.6.1.7.1. Implantação do Workload Security e XDR para 10 servidores.
4.9.6.1.7.2. Treinamento Hands On.
4.9.6.1.8. Fase de Execução pelo Email Security Standard:
4.9.6.1.8.1. Implantação do Email Security Standard para 1 gateway de correio eletrônico e até 2 domínios;
4.9.6.1.8.2. Passagem de conhecimento para a equipe da CONTRATANTE para utilização do sistema;
4.9.6.1.8.3. Definição de política de proteção;
4.9.6.1.8.4. Treinamento Hands On.
4.9.6.1.9. Fase de Execução do Cloud App Security (CAS) e XDR integrado ao Vision One e a sandbox;
4.9.6.1.9.1. Implantação do Cloud App Security para 1 provedor de serviço em nuvem, integrando caixas de correio eletrônico, armazenamento em nuvem e colaboração;
4.9.6.1.9.2. Ativação do XDR;
4.9.6.1.9.3. Passagem de conhecimento para a equipe da CONTRATANTE para utilização do sistema;

4.9.6.1.9.4. Definição de política de proteção;
4.9.6.1.9.5. Treinamento Hands On.

4.9.6.2. Fase de Execução para o Deep Discovery Inspector e XDR, integrado ao Vision One e Sandbox:
4.9.6.2.1.1. Instalação do Deep Discovery Inspector com a versão estável mais atualizada;
4.9.6.2.1.2. Ativação do XDR para Deep Discovery Inspector para a versão mais atualizada;
4.9.6.2.1.3. Passagem de conhecimento para a equipe da CONTRATANTE para utilização do sistema;
4.9.6.2.1.4. Definição de política de inspeção de rede;
4.9.6.2.1.5. Treinamento Hands On.

4.9.6.3. Fase de Execução para o File Storage:
4.9.6.3.1.1. Instalação do File Storage para a versão estável mais atualizada;
4.9.6.3.1.2. Passagem de conhecimento para a equipe da CONTRATANTE para utilização do sistema;
4.9.6.3.1.3. Treinamento Hands On.

4.9.6.4. Fase de Execução para o Conformity:
4.9.6.4.1.1. Instalação do Conformity para a versão estável mais atualizada;
4.9.6.4.1.2. Passagem de conhecimento para a equipe da CONTRATANTE para utilização do sistema;
4.9.6.4.1.3. Treinamento Hands On.

4.9.6.5. Fase de Encerramento:
4.9.6.5.1.1. Reunir as equipes CONTRATADA e CONTRATANTE para alinhamento de atividades pendentes, caso existam;
4.9.6.5.1.2. Analisar e encerrar atividades restantes;
4.9.6.5.1.3. Homologar o projeto;
4.9.6.5.1.4. Documentar as oportunidades de melhoria do processo.

4.9.7. Detalhamento do Serviço de Suporte Técnico Especializado na solução TRENDMICRO

4.9.7.1. A CONTRATADA deverá prestar suporte técnico no ambiente TRENDMICRO envolvendo as soluções de Apex One SaaS, XDR para Apex One, Apex central, Vulnerability Protection, Application Control, Workload Security, Email Security Standard, Cloud App Security, XDR para Cloud App Security, Deep Discovery Inspector, XDR para Deep Discovery Inspector, Cloud One File Storage, Cloud One Container Security, Cloud One Conformity;

4.9.7.2. Deverá ser prestado suporte reativo na modalidade 8X5X12 remotamente e em horário comercial;

4.9.7.3. Os chamados de suporte que não puderem ser resolvidos diretamente pela empresa contratada devem ser escalados para o fabricante. O acompanhamento do chamado escalado para o fabricante, e a alimentação do chamado é responsabilidade da empresa contratada.

4.9.7.4. Deverá ser prestado um suporte proativo envolvendo as seguintes atividades:

4.9.7.4.1. Diagnóstico especializado para a solução de endpoint e gateway de correio envolvendo: Apex One SaaS, Apex Central e Email Security Standard com a periodicidade anual. Esse relatório deverá verificar a conformidade das configurações das tecnologias em relação às boas práticas de mercado e as recomendações do fabricante, para orientar sobre a melhoria contínua das configurações das ferramentas de proteção

4.9.7.4.2. Diagnóstico especializado para a solução de Workload Security com a periodicidade anual. Esse relatório deverá verificar a conformidade das configurações das tecnologias em relação às boas práticas de mercado e as recomendações do fabricante, para orientar sobre a melhoria contínua das configurações das ferramentas de proteção

4.9.7.4.3. Apresentação trimestral de indicadores e métricas de cibersegurança através do Vision One, com visão gerencial do ambiente cibernético e orientação a respeito de possíveis melhorias.

4.9.7.4.4. Gerenciamento remoto mensal para verificação da saúde das tecnologias implantadas:
- Vision One
- Apex Central SaaS
- Apex One SaaS, Vulnerability Protection, Application Control
- Email Security Standard
- Cloud App Security
- Cloud ONe Workload Security
- Deep Discovery Inspector

4.9.7.4.5. Monitoramento de Ameaças e Vulnerabilidades através do Vision One e das tecnologias integradas para 14.200 endpoints pelo período de 24 meses;

4.9.7.4.6. Monitoramento proativo para verificação das ameaças, vulnerabilidades e atividades suspeitas registradas no Vision One para orientação ou tomada de ações necessárias para evitar a ocorrência de incidentes;

4.10. Requisitos da Contratada

4.10.1. A CONTRATADA deverá possuir os seguintes requisitos:

4.10.1.1. Fazer uso Plataforma de Gestão Estratégica de Segurança da Informação através de software que utilize os dados da solução de proteção contra ameaças digitais e faça diagnósticos especializados, apontando melhorias e recomendações com relação as melhores práticas do fabricante. A comprovação das funcionalidades citadas deve ser feita através de carta do desenvolvedor ou representante do software;

4.10.2. No início da prestação dos serviços, a CONTRATADA deverá possuir em seu portfólio, profissionais com, no mínimo, as seguintes certificações:

4.10.2.1. Profissional com certificação Apex One Certified Professional. A comprovação deve ser feita através de certificado do fabricante;
4.10.2.2. Profissional com certificação Deep Discovery Advanced Threat Detection. A comprovação deve ser feita através de certificado do fabricante;
4.10.2.3. Profissional com certificação Deep Security 20. A comprovação deve ser feita através de certificado do fabricante;
4.10.2.4. Profissional com certificação CISM (Certified Information Security Manager) da ISACA, comprovado através de certificado ISACA.
4.10.2.5. Profissional com certificação em Sistema de Gestão em segurança da Informação ISO/IEC 27001 (Auditor Lider), comprovado através de certificado emitido;
4.10.2.6. Profissional com certificação Cybersecurity Foundation ISO/IEC 27032 v2;
4.10.2.7. Profissional com certificação Cybersecurity Framework Foundation – NIST;
4.10.2.8. Profissional com certificação Trend Micro Cloud One Essentials;
4.10.2.9. Profissional com certificação Trend Micro Vision One Essentials;
4.10.2.10. Profissional com certificação Trend Micro Vision One for Administrator;
4.10.2.11. Profissional com certificação Trend Micro Threat Expertise;
4.10.2.12. Profissional com certificação Trend Micro Apex Central for Administrators;
4.10.2.13. Profissional com certificação Trend Micro Apex One Technical Track;
4.10.2.14. Profissional com certificação Trend Micro Vision One Technical Track;

As certificações profissionais serão auditadas na iniciação dos serviços;

5. MODELOS (TEMPLATES) A SEREM UTILIZADOS NA CONTRATAÇÃO

Os anexos a seguir contêm os modelos de:

ANEXO II – MODELO DE PROPOSTA COMERCIAL

ANEXO II – MODELO DA PROPOSTA COMERCIAL

Modelo da proposta

Nome Fantasia:			
Razão Social:			
CNPJ:		Inscrição Estadual:	
Endereço:		Cidade:	
Estado:	CEP:	Telefone:	Fax:

Prezados Senhores,

Após examinar todas as cláusulas e condições estipuladas no Edital em referência, apresentamos nossa proposta nos termos consignados no mencionado ato convocatório e seus anexos, com os quais concordamos plenamente.

Nossa proposta é válida por 90 (noventa) dias, contados da data de sua assinatura, sendo o preço ofertado firme e irreajustável durante o seu prazo de validade.

Informamos que estão inclusos nos preços ofertados todos os tributos, custos e despesas diretas ou indiretas, sendo de nossa inteira responsabilidade, ainda, os que porventura venham a ser omitidos na proposta ou incorretamente cotados.
O valor global de nossa proposta, conforme a tabela a seguir, é de R$_____ (por extenso):

ID	TÓ-PICO	ITEM	DESCRIÇÃO DO ITEM	Part Number	QTD.	Valor Unitário	Valor Total
1	4.3	Software de segurança para usuário final, contendo ambiente isolado e seguro para teste de novas ameaças, com visibilidade, detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Smart Protection Complete com detecção e resposta – 24 meses meses	CTNA0045 CTRA0045	14.200	R$ -	R$ -
			Apex One Sandbox as a Service Add-on to Apex One – 24 meses – 24 meses	ADNA0018 ADRA0015			
			Vision One XDR- 24 meses	VONA0000			
2	4.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One - Workload Security with XDR – 24 meses	CXNI0004 CXRI0004	1.001	R$ -	R$ -
			Service One Complete endpoint e Workload– 24 meses	SYNN0012 SYRN0012			
3	4.5	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante 24 (vinte e quatro) meses.	Deep Discovery Inspector Series 4000: 4Gbps SW+HW Appliance – 24 meses Deep Discovery Inspector 4000 Series Hardware	DDNA0033 DDRA0029 DDNA0019	1	R$ -	R$ -
			Vision One XDR- 24 meses	VONA0000			
			Service One Complete Network– 24 meses	SYN30000 SYR30000			
4	4.6	Solução de proteção para serviços em nuvem com validação de melhores práticas, incluindo garantia, atualização de versão e	Trend Micro Cloud One Conformity – 24 meses	CXNA0048 CXRA0048	10	R$ -	R$ -

		suporte especializado do fabricante por 24 (vinte e quatro) meses					
5	4.7	Solução de proteção para áreas de armazenamento de arquivos em nuvem, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One File Storage Security per bucket/blob- 24 meses	CXNA0027 CXRA0027	10	R$ -	R$ -
6	4.8	Treinamento oficial do fabricante	Voucher de Treinamento Oficial	TRNN1041	6	R$ -	R$ -
7	4.9	Gerenciamento especializado, proativo, preventivo e corretivo de ameaças por 24 (vinte e quatro) meses	Serviço de suporte especializado para diagnósticos, ajustes, configurações, migrações e implementação da solução a ser fornecida	Serviço Mensal	24	R$ -	R$ -
VALOR GLOBAL					**R$**		

Declaramos que nos preços ofertados estão inclusos tributos, emolumentos, encargos, contribuições fiscais e parafiscais, bem como todos os custos que venham a incidir sobre o fornecimento e a execução dos serviços.

Prazo de validade da proposta 90 dias

Salvador _____de _____ de 20__.

_____

RAZÃO SOCIAL

CNPJ

NOME DO REPRESENTANTE LEGAL

E ASSINATURA

ANEXO III – MODELO DE TERMO DE CONFIDENCIALIDADE

ANEXO AO CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA E A EMPRESA .....
(Pregão Eletrônico nº __/__ – Processo n° TJ-ADM-____/_____)

TERMO DE CONFIDENCIALIDADE SOBRE A SEGURANÇA DA INFORMAÇÃO

O ESTADO DA BAHIA, pessoa jurídica de direito público, inscrito no CNPJ/MF sob o nº 13.937.032/0001- 60, por intermédio do **TRIBUNAL DE JUSTIÇA DA BAHIA**, órgão do Poder Judiciário, inscrito no CNPJ/MF sob nº 13.100.722/0001-60, com sede e foro nesta cidade do Salvador, Estado da Bahia, na Quinta Avenida, nº 560, Centro Administrativo da Bahia – CAB, representado por..... adiante denominada simplesmente **CONTRATANTE**, e, do outro lado,....., inscrita no CNPJ sob nº....., doravante designada simplesmente **CONTRATADA**, representada por …....., inscrito no CPF/MF sob nº …....., resolvem, tendo em vista o constante do **PA nº …….....**com arrimo nas normas pertinentes da Lei Estadual nº 9.433/05 e, no que couber, na Lei Federal nº 8.666/93 e demais dispositivos legais aplicáveis, e tendo em vista o constante no **PA nº TJ-ADM-2022/19737**, e sempre que em conjunto referidas como PARTES para efeitos deste TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO, doravante denominado simplesmente TERMO, e,

CONSIDERANDO que, em razão do atendimento à exigência do contrato Nº ..., celebrado pelas PARTES, doravante denominado CONTRATO, cujo objeto é a ....., mediante condições estabelecidas pelo **CONTRATANTE**;

CONSIDERANDO que o presente TERMO vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de INFORMAÇÕES, que a .....NOME DA EMPRESA..... tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, conforme tipificado no Art.325 do Decreto – Lei 2.848/1940 (Código Penal Brasileiro), sobre todo e qualquer assunto de interesse do **CONTRATANTE** de que a .....NOME DA EMPRESA..... tomar conhecimento em razão da execução do CONTRATO, respeitando todos os critérios estabelecidos aplicáveis às INFORMAÇÕES;

O **CONTRATANTE** estabelece o presente TERMO mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO
O objeto deste TERMO é prover a necessária e adequada proteção às INFORMAÇÕES do **CONTRATANTE**, principalmente aquelas classificadas como CONFIDENCIAIS**,** em razão da execução do CONTRATO celebrado entre as PARTES.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS
a) As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer INFORMAÇÕES reveladas pelo **CONTRATANTE;**
b) A .....NOME DA EMPRESA..... se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer INFORMAÇÕES que venham a ser fornecidas pelo **CONTRATANTE**, a partir da data de assinatura deste TERMO, devendo ser tratadas como INFORMAÇÕES CONFIDENCIAIS, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo **CONTRATANTE**;
c) A .....NOME DA EMPRESA..... se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das INFORMAÇÕES do **CONTRATANTE**;
d) O **CONTRATANTE**, com base nos princípios instituídos na Segurança da Informação, zelará para que as INFORMAÇÕES que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela .....NOME DA EMPRESA.....
e) O **CONTRATANTE** pode, sem aviso prévio, restringir ou bloquear o acesso à Web Sites, serviços da Internet ou download de arquivos e examinar o conteúdo das mensagens de correio eletrônico, arquivos em computadores, cache de navegadores Web, bookmarks, histórico de sites visitados, configurações dos softwares e outras informações armazenadas ou transmitidas pelos seus computadores;
f) A .....NOME DA EMPRESA.....obriga-se a preservar o sigilo das senhas das contas dos usuários, não as ceder nem facilitar a sua descoberta, sob qualquer pretexto, bem como não utilizar contas e senhas pertencentes a outros servidores.

CLÁUSULA TERCEIRA – DAS LIMITAÇÕES DA CONFIDENCIALIDADE
As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:
a) Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES;
b) Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
c) Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as PARTES cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES ADICIONAIS
a) A .....NOME DA EMPRESA..... se compromete a utilizar as INFORMAÇÕES reveladas exclusivamente para os propósitos da execução do CONTRATO;
b) A .....NOME DA EMPRESA..... se compromete a não efetuar qualquer cópia das INFORMAÇÕES sem o consentimento prévio e expresso do **CONTRATANTE**;
b1) O consentimento mencionado na alínea "b", entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das PARTES;
c) A .....NOME DA EMPRESA..... se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste TERMO e da natureza confidencial das INFORMAÇÕES do **CONTRATANTE**;
d) A .....NOME DA EMPRESA..... deve tomar todas as medidas necessárias à proteção das INFORMAÇÕES do **CONTRATANTE**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo **CONTRATANTE**;
e) Cada PARTE permanecerá como única proprietária de todas e quaisquer INFORMAÇÕES eventualmente reveladas à outra parte em função da execução do CONTRATO;
f) O presente TERMO não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual;
g) Os produtos gerados na execução do CONTRATO, bem como as INFORMAÇÕES repassadas à .....NOME DA EMPRESA....., são de única e exclusiva propriedade intelectual do **CONTRATANTE**;
h) A .....NOME DA EMPRESA..... f**irmará acordos por escrito com cada um de seus empregados e consultores ligados direta ou indiretamente ao CONTRATO, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento, entregando uma via ao CONTRATANTE;**
i) A .....NOME DA EMPRESA..... obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às INFORMAÇÕES que venham a ser reveladas durante a execução do CONTRATO;
j) A .....NOME DA EMPRESA..... se compromete a envidar todos os esforços para preservar a confidencialidade das informações, adotando práticas de trabalho seguras quanto ao manuseio, armazenamento, transporte, impressão, transmissão e, quando for o caso, destruição de informações pertencentes ao **CONTRATANTE;**
k) A .....NOME DA EMPRESA..... se compromete a estar engajada na promoção de Segurança da Informação, incorporando as suas recomendações às atividades diárias do trabalho;
l) A .....NOME DA EMPRESA..... se compromete a notificar à Área de Segurança da Informação do **CONTRATANTE** em caso de divulgação ou suspeita de divulgação, acidental ou intencional, de informações pertencentes ao **CONTRATANTE**, bem como a descoberta de fragilidades de sistemas ou processos que possam propiciar a quebra de confidencialidade, disponibilidade ou integridade das informações.

CLÁUSULA QUINTA – DO RETORNO DE INFORMAÇÕES
Todas as INFORMAÇÕES reveladas pelas PARTES permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

CLÁUSULA SEXTA – DA VIGÊNCIA
O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura, até 5 (cinco) anos após o término do CONTRATO, e persiste após o término da atividade, mudança de função ou de encerramento do vínculo empregatício com a empresa.

CLÁUSULA SÉTIMA – DAS PENALIDADES
A quebra do sigilo e/ou da confidencialidade, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO firmado entre as PARTES. Neste caso, a .....NOME DA EMPRESA....., estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS
a) Este TERMO constitui vínculo indissociável ao CONTRATO, que é parte independente e regulatória deste instrumento;

b) O presente TERMO constitui acordo entre as PARTES, relativamente ao tratamento de INFORMAÇÕES, principalmente as CONFIDENCIAIS, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas PARTES em ações feitas direta ou indiretamente;
c) Surgindo divergências quanto à interpretação do pactuado neste TERMO ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa-fé, e, as preencherão com estipulações que deverão corresponder e resguardar as INFORMAÇÕES do **CONTRATANTE**;
d) O disposto no presente TERMO prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à confidencialidade de INFORMAÇÕES;
e) A omissão ou tolerância das PARTES, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA NONA - DO FORO
As partes elegem foro da Comarca de Salvador - BA, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, as partes firmam o presente instrumento em 2 (duas) vias de igual teor e um só efeito, juntamente com as testemunhas abaixo identificadas.

Salvador, ___ de _____ de 2023.

_____
TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA
Presidente do Tribunal de Justiça do Estado da Bahia

_____
(nome da empresa)
(nome e assinatura do representante legal –confirmar poderes no estatuto social ou procuração) (qualidade do representante legal –sócio-gerente, diretor, procurador)
(nome e assinatura do preposto)

Testemunhas:

Nome: _____
CPF: _____

Nome: _____
CPF: _____

ANEXO IV – MODELO DE TERMO DE DESIGNAÇÃO DE PREPOSTO

ANEXO AO CONTRATO DE ..... QUE ENTRE SI CELEBRAM …....., ., E A EMPRESA .....

(Pregão Eletrônico nº __/__ – Processo n° TJ-ADM-_____/_____)

Termo de Designação de Preposto

Contrato n°.....
Objeto: .....
Por meio deste instrumento, a (nome da empresa) nomeia e constitui seu(sua) preposto(a), o(a) Sr.(a) (nome do preposto), carteira de identidade n°....., expedida pela ....., inscrito(a) no Cadastro de Pessoas Físicas (CPF) sob o n° ....., com endereço ....., para exercer a representação legal junto ao Tribunal de Justiça do Estado da Bahia, com poderes para receber ofícios, representar a contratada em reuniões e assinar respectivas atas – obrigando a contratada nos termos dela constantes, receber solicitações e orientações para o cumprimento do contrato, notificações de descumprimento, de aplicação de penalidades, de rescisão, de convocação ou tomada de providências para ajustes e aditivos contratuais, e todas as demais que imponham, ou não, a abertura de processo administrativo ou prazo para a contratada responder ou tomar providências, e para representá-la em todos os demais atos que se relacionem à finalidade específica desta nomeação, que é a condução do contrato acima identificado.

Salvador, ... de ..... de 2023.
(nome da empresa)

{nome e assinatura do representante legal–confirmar poderes no estatuto social ou procuração) (qualidade do representante legal–sócio-gerente, diretor, procurador)

(nome e assinatura do preposto)

ANEXO V - MODELO DE DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DA PROPOSTA

[Identificação completa do representante da licitante], como representante devidamente constituído de [Identificação completa da licitante], doravante denominada LICITANTE, para fins de participação no certame licitatório acima identificado, declaro, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

(a) a proposta apresentada para participar desta licitação foi elaborada de maneira independente por mim e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato desta licitação, por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta elaborada para participar desta licitação não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato desta licitação, por qualquer meio ou por qualquer pessoa;

(c) que não tentei, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato desta licitação quanto a participar ou não dela;

(d) que o conteúdo da proposta apresentada para participar desta licitação não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato desta licitação antes da adjudicação do objeto;

(e) que o conteúdo da proposta apresentada para participar desta licitação não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante do órgão licitante antes da abertura oficial das propostas; e
(f) que estou plenamente ciente do teor e da extensão desta declaração e que detenho plenos poderes e informações para firmá-la.

Salvador, _____de _____ de 20____.

_____
NOME/RAZÃO SOCIAL CPF/ CNPJ
REPRESENTANTE LEGAL / ASSINATURA

ANEXO VI - MODELO DE DECLARAÇÃO DE RESPONSABILIDADE

(a ser apresentada pelo arrematante de cada lote)

Referência: PREGÃO ELETRÔNICO **__/20__ - Tribunal de Justiça do Estado da Bahia**
Data: ___/___/_____
Empresa Licitante:_____
CNPJ: _____

(*Nome do Licitante*), por intermédio de seu representante legal, **DECLARA**, sob as penas da Lei, que conhece e aceita, em todos os seus termos e sem restrição, o Edital da referida licitação, comprometendo-se a cumprir com todas as exigências nele determinadas.

Salvador _____de _____ de 20____.

_____
RAZÃO SOCIAL/ CNPJ/NOME DO REPRESENTANTE LEGAL/ E ASSINATURA
Nome: _____Cargo / Função: _____
Telefone: _____ E-mail: _____

OBS.: Esta declaração deve ser emitida em papel timbrado da Empresa Licitante.

ANEXO VII - MODELO DE DECLARAÇÃO DE ENQUADRAMENTO E DE ATENDIMENTO ÀS EXIGÊNCIAS DE HABILITAÇÃO

Para fins do tratamento diferenciado e favorecido de que cogita a Lei Complementar nº 123/06, alterada pela Lei Complementar nº147/2014, a licitante deverá apresentar, anexo a esta Declaração, a Certidão expedida pela Junta Comercial, no caso de empresas ali registradas, para comprovação da condição de microempresa ou empresa de pequeno porte, (Art. 8º da Instrução Normativa nº 103/2007 do Departamento Nacional de Registro do Comércio) ou Certidão específica do Registro Civil das Pessoas Jurídicas, nos demais casos.

O enquadramento do empresário ou da sociedade simples ou empresária como microempresa ou empresa de pequeno porte bem como o seu desenquadramento não implicarão alteração, denúncia ou qualquer restrição em relação a contratos por elas anteriormente firmados.

Declaramos, para fins do tratamento diferenciado e favorecido de que cogita a Lei Complementar nº 123/06, que:

( ) NÃO ESTAMOS ENQUADRADOS na condição de microempresa, nem de empresa de pequeno porte.

( ) Estamos enquadrados, na data designada para o início da sessão pública, na condição de MICROEMPRESA e que não estamos incursos nas vedações a que se reporta o §4º do art. 3º da Lei complementar nº 123/06, alterada pela Lei Complementar nº147/2014.

( ) Estamos enquadrados, na data designada para o início da sessão pública, na condição de EMPRESA DE PEQUENO PORTE e que não estamos incursos nas vedações a que se reporta o §4º do art. 3º da Lei complementar nº 123/06, alterada pela Lei Complementar nº147/2014.

No que concerne ao conhecimento e atendimento às exigências de habilitação, declaramos:

( ) Para os efeitos do inciso II do art. 120, em face do quanto disposto no inc. V do artigo 184, do mesmo diploma estadual, o pleno conhecimento e atendimento às exigências de habilitação, cientes das sanções factíveis de serem aplicadas a teor do art. 186 do mesmo diploma e da obrigatoriedade de declarar ocorrências posteriores.

( ) Para os efeitos do §1º do art. 43 da Lei complementar nº 123/06, haver restrição na comprovação da nossa regularidade fiscal, a cuja regularização procederemos no prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento da declaração do vencedor do certame, prorrogáveis, a critério da Administração Pública, cientes de que a não-regularização da documentação, no prazo previsto implicará decadência do direito à contratação, sem prejuízo das sanções previstas na Lei Estadual nº 9.433/05, especialmente a definida no art. 192, inc. I.

O signatário declara neste ato, sob as penas da legislação aplicável, que é representante legal da entidade e assume o compromisso de informar, imediatamente, ao órgão competente e à entidade contratante, qualquer alteração relativa ao enquadramento, reenquadramento ou desenquadramento da situação acima declarada.

Salvador _____de _____ de 2023.

_____
RAZÃO SOCIAL, CNPJ, NOME DO REPRESENTANTE LEGAL E ASSINATURA

ANEXO VIII - MODELO DE DECLARAÇÃO DE CUMPRIMENTO AO ART. 1º DO DECRETO JUDICIÁRIO Nº 95/14 e Resolução do CNJ nº 229/16)

Declaramos, sob pena de Lei, que a empresa .....(razão social/CNPJ) ..... NÃO INCORRE em nenhuma das hipóteses deliberadas no art. 1º do Decreto Judiciário nº 95/14, bem como da Resolução do CNJ nº 229/16.

Salvador _____de _____ de 2023.

_____

RAZÃO SOCIAL, CNPJ, NOME DO REPRESENTANTE LEGAL E ASSINATURA

ANEXO IX - MODELO DE PROCURAÇÃO PARA A PRÁTICA DE ATOS CONCERNENTES AO CERTAME

Através do presente instrumento, nomeamos e constituímos o(a) Senhor(a) ....., (nacionalidade, estado civil, profissão), portador do Registro de Identidade nº ....., expedido pela ....., devidamente inscrito no Cadastro de Pessoas Físicas do Ministério da Fazenda, sob o nº ....., residente à rua ....., nº ..... como nosso mandatário, a quem outorgamos amplos poderes para praticar todos os atos relativos ao procedimento licitatório **PREGÃO ELETRÔNICO nº XX/20XX** indicado acima, conferindo-lhe poderes para:.....(apresentar proposta de preços, formular ofertas e lances, interpor recursos e desistir deles, contra-arrazoar, assinar contratos, negociar preços e demais condições, confessar, firmar compromissos ou acordos, receber e dar quitação, apresentar defesa prévia e praticar todos os demais atos pertinentes ao certame, etc).

Salvador _____de _____ de 2023.

_____

RAZÃO SOCIAL/ CNPJ/NOME DO REPRESENTANTE LEGAL/ E ASSINATURA

ANEXO X - MODELO DE DECLARAÇÃO DE PLENO CONHECIMENTO E DE VERACIDADE DOS DOCUMENTOS

Modalidade de Licitação	Número

Em cumprimento ao art. 120, II da Lei estadual nº 9.433/05 e ao art. 18, §4º do Decreto nº 19.896/20, e em face do quanto disposto no art. 184, inc. V, e no art. 195 da Lei estadual nº 9.433/05, declaro:

( ) o **pleno conhecimento e atendimento às exigências de habilitação**.

[ou]
[exclusivamente para microempresas e empresas de pequeno porte beneficiárias da Lei Complementar nº 123/06]

( ) o **pleno conhecimento e atendimento às exigências de habilitação**, ressalvada, na forma do §1º do art. 43 da Lei complementar nº 123/06, a existência de restrição fiscal e/ou trabalhista.

Declaro, ainda, a veracidade dos documentos por mim apresentados, sob as penas da lei.

Salvador _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

ANEXO XI - MODELO DE DECLARAÇÃO DE DESIMPEDIMENTO DE LICITAR E/OU CONTRATAR

Declaramos, sob pena de Lei, que a empresa .....(razão social/CNPJ) ..... não está impedida de licitar ou contratar com a Administração direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, abrangendo inclusive as entidades com personalidade jurídica de direito privado sob controle do poder público e as fundações por ele instituídas ou mantidas (art. 185, III, da Lei Estadual nº 9.433/05).

Salvador _____de _____ de 2023.

_____

RAZÃO SOCIAL/ CNPJ/NOME DO REPRESENTANTE LEGAL/E ASSINATURA

ANEXO XII – MODELO DE MINUTA DO CONTRATO

INSTRUMENTO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI, CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA E ..... NA FORMA ABAIXO:

O ESTADO DA BAHIA, pessoa jurídica de direito público, inscrito no CNPJ/MF sob o nº 13.937.032/0001-60, por intermédio do **TRIBUNAL DE JUSTIÇA DA BAHIA,** órgão do Poder Judiciário, inscrito no CNPJ/MF sob nº 13100722/0001-60, com sede e foro nesta cidade do Salvador, Estado da Bahia, na Quinta Avenida, nº 560, Centro Administrativo da Bahia – CAB, representado pelo seu Presidente, **DES. ,** adiante denominado simplesmente **CONTRATANTE**, e, do outro lado,....., inscrita no CNPJ sob nº....., situada ….., doravante designada simplesmente **CONTRATADA**, representada por ….., inscrito no CPF/MF sob nº ….., situada …….., resolvem, tendo em vista o constante do **PA nº TJ-ADM-2022/19737**, relativo ao **Pregão Eletrônico nº 068/2022**, com arrimo nas normas pertinentes da Lei Estadual nº 9.433/05 e, no que couber, na Lei Federal nº 8.666/93, Lei nº 12.846/2013, Lei nº 13.709/2018 e demais dispositivos legais aplicáveis, ajustando e reciprocamente aceitando as seguintes cláusulas e condições:

DO OBJETO

CLÁUSULA PRIMEIRA – Habilitada nos termos do **Pregão Eletrônico nº 068/2022,** devidamente homologada em ....., e publicação no DPJ, edição de....., obriga-se a **CONTRATADA** a prestar os serviços referentes à solução de segurança da informação, composta de software de segurança para usuário final e cargas de trabalho híbridas, proteção contra ameaças avançadas incluindo fornecimento de *appliance*, proteção contra ameaças de nuvem e gerenciamento de conformidade, com detecção e resposta e gerenciamento proativo e corretivo das soluções, para o Tribunal de Justiça do Estado da Bahia, tudo em perfeita observância às condições e especificações constantes do EDITAL, seus ANEXOS e PROPOSTA VENCEDORA, os quais passam a integrar o presente instrumento de modo indissociável.

Parágrafo primeiro: O Tribunal de Justiça do Estado da Bahia não aceitará a subcontratação de outras empresas nem a formação de consórcio para a prestação dos serviços licitados, devendo uma única empresa assumir a responsabilidade integral pela execução.

Parágrafo segundo: Será admitida, caso necessário, a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que: sejam observados, pela nova pessoa jurídica, todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado; e haja a anuência expressa da Administração à continuidade do contrato.

DO REGIME DE EXECUÇÃO

CLÁUSULA SEGUNDA - O objeto deste contrato será prestado pelo regime de empreitada por preço unitário.

DAS OBRIGAÇÕES DA CONTRATADA

CLÁUSULA TERCEIRA – Obriga-se a Contratada a:

a) Fornecer o objeto adjudicado em estrita conformidade com as especificações, quantidades, prazos e demais condições estabelecidas no Edital e seus anexos;
b) Participar de reunião de alinhamento a ser realizada em data e horário a ser definido pelo CONTRATANTE, nos termos estabelecidos no Item 3.3.1 – Reunião de Alinhamento DO Anexo I – Termo de Referência;
c) Designar e apresentar o preposto do contrato no ato da reunião de alinhamento;
d) Estar disponível para realizar reuniões periódicas com o CONTRATANTE, podendo este último, em atenção às circunstâncias específicas, dispensar reuniões programadas ou convocar, em caso de necessidade, reuniões extraordinárias, às que um representante da CONTRATADA deve comparecer no prazo máximo de dois dias úteis;
e) A CONTRATADA deverá responsabilizar-se solidariamente pela execução completa e satisfatória do fornecimento e dos serviços associados, por meio do gerenciamento dos seus recursos humanos e técnicos, assim como, não poderá se eximir dessa obrigação, ainda que parcialmente, atribuindo a ela quaisquer falhas ou deficiências à imperícia de pessoal ou a erros de especificações;
f) Quando do comparecimento às dependências da CONTRATANTE, promover, por sua conta e risco, o transporte de seus empregados, materiais e utensílios necessários envolvidos nas atividades motivo desta contratação, até às instalações do CONTRATANTE;
g) Quando do comparecimento às dependências da CONTRATANTE, o preposto e os colaboradores da CONTRATADA deverão estar devidamente identificados com crachá no qual conste seu nome, o nome da empresa e a função desempenhada;
h) Respeitar e fazer com que seus empregados respeitem as normas de segurança, disciplina e demais regulamentos vigentes no Poder Judiciário da Bahia, bem como atentar para as regras de cortesia no local onde serão executados os serviços objeto do contrato;

i) Facilitar por todos os meios a seu alcance a ampla ação fiscalizadora do CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem dirigidas;
j) Utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas no contrato, edital e seus anexos;
k) Pagar os salários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços contratados, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vale-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhes defeso invocar a existência deste contrato para eximir-se destas obrigações ou transferi-las para o CONTRATANTE;
l) Manter o sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do Contrato, respeitando todos os critérios estabelecidos no Termo de Confidencialidade anexo ao certame;
m) Promover, caso necessário, a intermediação junto ao fabricante, para garantir o suporte remoto, o fornecimento de manuais e o acompanhamento necessário para a transferência tecnológica e todas as demais opções de interação com a CONTRATANTE, em sua língua nativa – Português do Brasil;
n) Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pelo Ministério do Trabalho e Emprego, por meio da Portaria nº 540/2004.
o) Não ter sido condenada, a contratada ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta a previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal Brasileiro; do Decreto nº 5.017/2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nos 29 e 105.

DAS OBRIGAÇÕES DO CONTRATANTE

CLÁUSULA QUARTA - Obriga-se o Contratante a:

a) Designar servidores para acompanhamento e fiscalização do contrato, conforme disposto no art. 16 da Resolução nº 182/2013 do Conselho Nacional de Justiça – CNJ e Norma Geral de Contratações do TJBA;
b) Exercer a fiscalização dos serviços, podendo recusar qualquer serviço que não esteja de acordo com as condições estabelecidas no Termo de Referência;
c) Assegurar-se da boa prestação dos serviços, verificando sempre seu bom desempenho;
d) Atestar, por intermédio de servidor especialmente designado, as notas fiscais referentes aos serviços e fornecimentos prestados de forma satisfatória;
e) Efetuar o pagamento devido à CONTRATADA, dentro do prazo estipulado, desde que cumpridas todas as formalidades e exigências contratuais;
f) Zelar para que, durante a vigência do contrato, sejam cumpridas as obrigações assumidas por parte da CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas.
g) Manter em arquivo, junto ao processo administrativo ao qual está vinculado o Termo de Referência, toda a documentação a ele pertinente;
h) Disponibilizar todas as informações necessárias para o desenvolvimento dos trabalhos;
i) Fornecer a infraestrutura necessária para o pleno funcionamento dos Serviços, seguindo as especificações técnicas fornecidas pela CONTRATADA e dentro das normas ABNT relacionadas. Entende-se como infraestrutura, os recursos computacionais necessários para a execução da plataforma;
j) Validar e aprovar os serviços executados, em conformidade com as regras e requisitos estabelecidos no ANS (Acordo de Níveis de Serviço), refletindo a qualidade entregue em conformidade com o IMR (Instrumento de Medição de Resultado);
k) Providenciar o acesso controlado dos profissionais da CONTRATADA ao ambiente de TI, incluindo bibliotecas de programas, políticas, normas, procedimentos, metodologias, bases de dados, ferramentas, de acordo com pré-requisitos definidos nas comunicações formais de demanda;
l) Aplicar as sanções conforme previsto no contrato;
m) Gerir e fiscalizar, quantitativa e qualitativamente, a execução das demandas por meio do acompanhamento das atividades desenvolvidas e resultados obtidos, observando os prazos e produtos acordados com vistas a efetuar eventuais ajustes e correções de rumo.

DO PREÇO

CLÁUSULA QUINTA: O **CONTRATANTE** pagará à **CONTRATADA**, pelos fornecimentos e serviços efetivamente entregues, os valores abaixo especificados:

ID	TÓ-PICO	ITEM	DESCRIÇÃO DO ITEM	Part Number	QTD.	Valor Unitário	Valor Total
1	4.3	Software de segurança para usuário final, contendo ambiente isolado e seguro para teste de novas ameaças, com visibilidade, detecção e resposta, incluindo garantia,	Trend Micro Smart Protection Complete com detecção e resposta – 24 meses meses	CTNA0045 CTRA0045	14.200	R$ -	R$ -
				ADNA0018			

		atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Apex One Sandbox as a Service Add-on to Apex One – 24 meses – 24 meses	ADRA0015			
			Vision One XDR- 24 meses	VONA0000			
2	4.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One - Workload Security with XDR – 24 meses	CXNI0004 CXRI0004	1.001	R$ -	R$ -
			Service One Complete endpoint e Workload– 24 meses	SYNN0012 SYRN0012			
3	4.5	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia, atualização de versão e suporte especializado do fabricante 24 (vinte e quatro) meses.	Deep Discovery Inspector Series 4000: 4Gbps SW+HW Appliance – 24 meses Deep Discovery Inspector 4000 Series Hardware	DDNA0033 DDRA0029 DDNA0019	1	R$ -	R$ -
			Vision One XDR- 24 meses	VONA0000			
			Service One Complete Network– 24 meses	SYN30000 SYR30000			
4	4.6	Solução de proteção para serviços em nuvem com validação de melhores práticas, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One Conformity – 24 meses	CXNA0048 CXRA0048	10	R$ -	R$ -
5	4.7	Solução de proteção para áreas de armazenamento de arquivos em nuvem, incluindo garantia, atualização de versão e suporte especializado do fabricante por 24 (vinte e quatro) meses	Trend Micro Cloud One File Storage Security per bucket/blob- 24 meses	CXNA0027 CXRA0027	10	R$ -	R$ -
6	4.8	Treinamento oficial do fabricante	Voucher de Treinamento Oficial	TRNN1041	6	R$ -	R$ -
7	4.9	Gerenciamento especializado, proativo, preventivo e corretivo de ameaças por 24 (vinte e quatro) meses	Serviço de suporte especializado para diagnósticos, ajustes, configurações, migrações e implementação da solução a ser fornecida	Serviço Mensal	24	R$ -	R$ -
VALOR GLOBAL					**R$**		

Parágrafo primeiro: Este contrato tem um valor global de R$ .....

Parágrafo segundo: Nos preços contratados estão incluídos todas e quaisquer despesas necessárias ao cumprimento do objeto desta licitação, tais como mão de obra, impostos, tributos, encargos e contribuições sociais, fiscais, parafiscais, fretes, seguros, transporte, estadia, alimentação e demais despesas inerentes, correrão por conta da CONTRATADA, não cabendo ao CONTRATANTE o reembolso de despesas com transporte, hospedagem e outros custos operacionais, não previstos no Edital e seus anexos, que devem ser de exclusiva responsabilidade da CONTRATADA..

DO PAGAMENTO

CLÁUSULA SEXTA - Os pagamentos devidos à **CONTRATADA** serão efetuados através de ordem bancária ou crédito em conta corrente, no prazo não superior a 08 (oito) dias úteis, contados da data da apresentação da fatura, após concluído o recebimento definitivo, em consonância com o disposto no art. 6º, § 5º; art. 8º, XXXIV; art. 79, XI, "a"; art. 154, V e art. 155, V da Lei estadual nº. 9.433/05.

a) O faturamento só poderá ser apresentado após a emissão do Termo de Recebimento Definitivo (TDR), indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao fornecimento e prestação dos serviços, acompanhado da documentação probatória relativa ao recolhimento dos impostos relacionados com a obrigação, obedecidos os prazos descritos no item **3.3.1 – Cronograma de Entrega dos Serviços do Anexo I – Termo de Referência do Edital.**

b) Devido à política global de venda do fabricante, para os itens de 01 a 05, componentes da solução, o

pagamento será efetuado em parcela única após Termo de Recebimento Definitivo a ser emitido para cada um dos itens.

c) Para o item 06 da solução, que ocorrerá sob demanda, o faturamento também será feito em parcela única, de acordo com o consumo, e só poderá ser apresentado após a CONTRATANTE emitir o TRD do respectivo item, indicando a realização e satisfação com os treinamentos entregues;

d) Para o item 07 da solução, o pagamento será realizado mensalmente, após verificados os critérios descritos nos itens 3.5 (Acompanhamento dos Prazos de Garantia e Níveis Mínimos de Serviço) e 3.6 (Instrumentos de Medição dos Serviços), ambos do Anexo I – Termo de Referência. Deverá ser apresentada uma Nota Fiscal para cada mês de serviço prestado.

e) Os faturamentos deverão ser apresentados **em notas fiscais de venda ou serviço**, de acordo com as características de cada objeto, e serão pagos por meio de ordem bancária ou crédito em conta corrente, em até 08 (oito) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, condicionado ao seu ateste pelo Gestor do Contrato, em consonância com o disposto no art. 6º, § 5º; art. 8º, XXXIV; art. 79, XI, "a"; art. 154, V e art. 155, V da Lei Estadual nº 9.433/05.

f) O valor global a ser pago à CONTRATADA deverá atender aos valores cotados na proposta vencedora.

g) A efetivação e aceite de quaisquer serviços não previstos só poderão ocorrer mediante aprovação formal do CONTRATANTE.

h) Na ocasião de ocorrência de erro na(s) nota(s) fiscal(s)/fatura(s) ou qualquer circunstância que impeça a liquidação da despesa, aquela será restituída ou será comunicada a irregularidade à CONTRATADA, ficando pendente de pagamento até que esta providencie as medidas saneadoras. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação e/ou a reapresentação do documento fiscal, não acarretando qualquer ônus para a CONTRATANTE;

i) A CONTRATANTE poderá deduzir do montante a pagar ou do montante depositado como garantia, quando for o caso, valores correspondentes a multas ou indenizações devidas pela CONTRATADA, decorrentes de penalidades aplicadas nos termos do Contrato e deste Termo de Referência;

j) Em hipótese alguma serão pagos serviços não contratados;

k) A CONTRATADA deverá apresentar nota fiscal correspondente ao objeto fornecido, reservando-se o CONTRATANTE o direito de não atestá-la para o pagamento se os dados nela constantes estiverem em desacordo com as especificações apresentadas neste Edital, ficando o pagamento suspenso até a regularização.

l) O atesto na nota fiscal é condição indispensável para o pagamento desta. Na ausência do gestor, o atesto será dado por gestor substituto.

m) O CNPJ constante da nota fiscal deverá ser o mesmo indicado na proposta, nota de empenho e vinculado à conta-corrente da CONTRATADA.

Parágrafo primeiro: Em havendo alguma pendência impeditiva do pagamento, a exemplo de erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como obrigações financeiras pendentes, decorrentes de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

Parágrafo segundo: A atualização monetária dos pagamentos devidos pelo **CONTRATANTE**, em caso de mora, será calculada considerando a data do vencimento da Nota Fiscal/Fatura e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE, *pro rata temporis*.

Parágrafo terceiro: Qualquer pagamento, somente será efetuado mediante apresentação da respectiva Nota Fiscal emitida em nome do Tribunal de Justiça do Estado da Bahia, acompanhada da Fatura correspondente.

Parágrafo quarto: O prazo referido no caput desta cláusula será interrompido na ocorrência de erros ou qualquer outra irregularidade na fatura apresentada, voltando o prazo de pagamento a ser contabilizado, na íntegra, depois de efetuadas as devidas correções.

Parágrafo quinto: A **CONTRATADA** deverá obedecer integralmente às disposições quanto à obrigatoriedade de emissão da Nota Fiscal por meio eletrônico, nos termos do Regulamento do ICMS Bahia, com as alterações contidas no Decreto Estadual nº 10.666 de 03/08/2006.

Parágrafo sexto: Nenhum pagamento isentará a CONTRATADA das responsabilidades contratuais, nem implicará em aprovação definitiva dos serviços executados, total ou parcialmente**.**

DA GARANTIA

CLÁUSULA SÉTIMA – Será exigida, como condição para a celebração do contrato, a prestação, pela **CONTRATADA**, de garantia **de 5% (cinco por cento)** sobre o preço global do objeto a ser contratado, no prazo máximo de 10 (dez) dias corridos da assinatura deste instrumento.

Parágrafo primeiro: A garantia será prestada em caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, pelo prazo equivalente ao deste contrato acrescido de mais três meses do término da vigência contratual.

I - Não será admitida a existência de cláusulas que restrinjam ou atenuem a responsabilidade do segurador ou fiador, nocaso de seguro-garantia ou fiança bancária (art. 136, §1º, II e III da Lei estadual nº 9.433/05).

Parágrafo segundo: O cálculo da atualização monetária do valor caucionado em dinheiro será feito aplicando-se o índice mais vantajoso para a Administração entre a data de retenção da caução e da devolução do seu valor.

Parágrafo terceiro: A liberação da garantia ou sua restituição se dará após o recebimento definitivo do objeto do contrato ou a comprovação de quitação de todas as obrigações trabalhistas e previdenciárias dos recursos humanos envolvi- dos na Prestação de Serviços, quando for o caso, inclusive garantidas eventuais demandas judiciais decorrentes da presente contratação, nos termos do Instrumento Contratual, e quando em dinheiro, atualizada monetariamente, deduzi- dos eventuais valores devidos ao **CONTRATANTE.**

Parágrafo quarto: A garantia será obrigatoriamente revista e complementada quando houver redução da sua representatividade percentual por variação econômica do contrato ou descontos de valores devidos ao **CONTRATANTE.**

Parágrafo quinto: No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

Parágrafo sexto: O valor da garantia permanecerá integral até o término da vigência do Contrato. Se o valor da garantia for utilizado, total ou parcialmente, pela **CONTRATANTE,** para compensação de prejuízo causado no decorrer da execução contratual por conduta da **CONTRATADA,** esta deverá proceder à respectiva reposição no prazo de 10 (dez) dias corridos, contados da data em que tiver sido notificada.

Parágrafo sétimo: A garantia responderá pelo inadimplemento das obrigações contratuais e multas impostas, independentemente de outras cominações legais.

DA FISCALIZAÇÃO E RECEBIMENTO DO OBJETO

CLÁUSULA OITAVA - Competirá ao CONTRATANTE proceder ao acompanhamento da execução do contrato, na forma do art. 154 da Lei estadual 9.433/05, ficando esclarecido que a ação ou omissão, total ou parcial, da fiscalização do CONTRATANTE não eximirá a CONTRATADA de total responsabilidade na execução do contrato.

Parágrafo primeiro - O adimplemento da obrigação contratual por parte da CONTRATADA ocorre com a efetiva prestação do serviço, a realização da obra, a entrega do bem, assim como qualquer outro evento contratual cuja ocorrência esteja vinculada à emissão de documento de cobrança, consoante o art. 8º, inc. XXXIV, da Lei estadual 9.433/05.

Parágrafo segundo - Cumprida a obrigação pela CONTRATADA, caberá ao CONTRATANTE proceder ao recebimento do objeto, a fim de aferir se os serviços ou fornecimentos foram efetuados, para efeito de emissão da habilitação de pagamento, conforme o art. 154, inc. V, e art. 155, inc. V, da Lei estadual 9.433/05.

Parágrafo terceiro - A emissão de aceite dos serviços pelo CONTRATANTE não exime a CONTRATADA da responsabilidade pela correção de erros porventura identificados, sem ônus adicional, durante a execução dos serviços e vigência contratual, conforme disposto no Art. 157 da Lei 9.433/2005. Surgindo deficiências durante a execução dos serviços e vigência contratual, o CONTRATANTE requererá, por escrito, a resolução dos problemas, ficando a CONTRATADA obrigada a providenciar, junto ao fabricante, a recomposição do nível de serviços condizente com as exigências desta contratação.

Parágrafo quarto: O TJBA designará servidor responsável para realizar o recebimento dos objetos, da seguinte forma:

a) TERMO DE RECEBIMENTO PROVISÓRIO: Para os itens de hardware: Deverão ser comprovadas as entregas desses objetos nas dependências do TJBA, no prazo definido no **item 3.3.1 - cronograma de entrega dos serviços** do Anexo I – Termo de Referência deste Edital.

a.1) Todas as comprovações serão aceitas em formato digital ou impresso, via *e-mail* ou presencialmente.

b) TERMO DE RECEBIMENTO DEFINITIVO: Os Termos de Recebimento Definitivo serão emitidos conforme a seguir:

I) Para os itens de *Software*: Os objetos deverão ser entregues através de carta emitida pelo fabricante, contendo as informações dos objetos contratados, o regime de suporte especificado no termo de referência, os dados de acesso do TJBA ao portal de suporte do fabricante, a vigência dos serviços contratados, os dados do cliente e do fabricante, e o registro informativo de que os produtos foram adquiridos através do licitante arrematante.
II) Para os itens de *Hardware*: Os objetos deverão ser instalados fisicamente no *Datacenter*, na sede do TJBA.
III) Para os itens de treinamento: Será atestado o recebimento dos itens em até 10 (dez) dias corridos, após a realização dos treinamentos previstos nesta contratação.
IV) Para os itens de prestação de serviços: Serão emitidos mensalmente, após cumpridos os requisitos descritos nos itens 3.5 (Acompanhamento dos Prazos de Garantia e Níveis Mínimos de Serviço), 3.6 (Instrumentos de Medição dos Serviços) e seus subitens, constantes do Anexo I – Termo de Referência.

b.1) Os **Termos de Recebimento Definitivo**, nos termos do Art. 161 da Lei Estadual nº 9.433/2005, serão emitidos em razão de parecer circunstanciado de servidor ou comissão designada pela autoridade competente, mediante termo assinado pelas partes, após as entregas das atividades descritas nesta cláusula, nos prazos indicados no item 3.3.1 – Cronograma de Entrega dos Serviços, sendo observado o disposto no art. 157 da mesma Lei.

b.2) A emissão de aceite dos serviços pelo CONTRATANTE não exime a CONTRATADA da responsabilidade pela correção de erros porventura identificados, sem ônus adicional.

Parágrafo quinto: Esgotado o prazo total para conclusão do recebimento definitivo sem qualquer manifestação do órgão ou entidade CONTRATANTE, considerar-se-á definitivamente aceito o objeto contratual, para todos os efeitos.

Parágrafo sexto: Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar a(s) nota(s) fiscal (is)/fatura(s) para pagamento.

Parágrafo sétimo: A administração indicará servidores (fiscal e suplente), por meio de portaria devidamente publicada, para acompanhar o presente objeto deste certame.

DOS PRAZOS

CLÁUSULA NONA – O contrato vigerá pelo período inicial de 24 (vinte e quatro) meses, contados a partir da data de sua assinatura, podendo ser prorrogado nos termos do Art. 140 da Lei Estadual nº 9.433/2005**.**

Parágrafo primeiro: A publicação resumida deste instrumento no Diário da Justiça Eletrônico é condição para a sua eficácia e validade, devendo ocorrer no prazo de até 10 (dez) dias corridos da sua assinatura.

Parágrafo segundo: A execução dos serviços será conforme item 3 – Detalhamento do Objeto e seus subitens do Anexo I - Termo de Referência e atenderá ao cronograma de entrega abaixo:

ID	Evento	Quando	Prazo em dias até	Quem
1	Assinatura do Contrato	Início	Não se aplica	Ambos
1.1	Emissão do Empenho	Após ID 1	Não se aplica	Contratante
2	Reunião de Alinhamento	Após ID 1	5 dias corridos	Ambos
3	Início do Serviço Gerenciamento mensal descrito no item 7	Após ID 2	Imediatamente	Ambos
4	Entrega dos itens de software 1,2,4, e 5	Após ID 1.1	15 dias corridos	Contratada
5	Emissão do Termo de Recebimento Definitivo (TRD) para itens 1,2,4,5	Após ID 4	10 dias corridos	Contratante
6	Entrega do *appliance* descrito no item 3	Após ID 1.1	60 dias corridos	Contratada
7	Emissão do Termo de Recebimento Provisório (TRP) para item 3	Após ID 6	5 dias corridos	Contratante

8	Instalação física do *appliance* descrito no item 3 no Datacenter	Após ID 7	10 dias corridos	Contratada
9	Emissão do Termo de Recebimento Definitivo (TRD) para itens 3	Após ID 8	10 dias corridos	Contratante

DA MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA – REAJUSTAMENTO E REVISÃO

CLÁUSULA DÉCIMA - Os preços são fixos e irreajustáveis durante a vigência inicial do contrato.

Parágrafo primeiro: Dentro do prazo de vigência, em caso de prorrogação do contrato mediante solicitação do CONTRATANTE, os valores contratados poderão ser reajustados, aplicando o ICTI (Índice de Custos de Tecnologia da Informação). Caso o índice estabelecido para reajuste venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação vigente.

DOS ILÍCITOS E PENALIDADES

CLÁUSULA DÉCIMA PRIMEIRA - A CONTRATADA cumprirá, rigorosamente as condições estabelecidas no edital e seus anexos e na proposta vencedora, para execução do objeto deste contrato, inclusive obrigações adicionais estabelecidas neste instrumento, sob pena de sujeitar-se às penalidades cabíveis.

Parágrafo primeiro: À CONTRATADA, na hipótese de inexecução contratual, seja parcial ou total, inclusive por atraso injustificado na execução do contrato, serão aplicadas, sem prejuízo da rescisão unilateral do contrato, a qualquer tempo, e outras cominações legais, MULTA DE MORA:

a) 10% (dez por cento) sobre o valor global do contrato, em caso de descumprimento total da obrigação principal;
b) caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado o percentual 10% (dez por cento) sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento ou serviço já realizado.
c) em caso de atraso no cumprimento da obrigação principal, será aplicado o percentual de 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento ou serviço não realizado e de,
d) 0,7% (sete décimos por cento) sobre o valor da parte do fornecimento ou serviço não realizado, por cada dia subsequente ao trigésimo.

Parágrafo segundo: Na hipótese de a contratada negar-se a efetuar o reforço da caução, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multa percentual de 2,5% (dois e meio por cento) incidente sobre o valor global do contrato.

Parágrafo terceiro: As multas previstas neste artigo não têm caráter compensatório e o seu pagamento não eximirá a contratada da responsabilidade por perdas e danos decorrentes das infrações cometidas.

Parágrafo quarto: A multa, aplicada após regular processo administrativo, será descontada da garantia do contratado faltoso, sendo certo que, se o seu valor exceder ao da garantia prestada – quando exigida, além da perda desta, a CONTRATADA responderá pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou, ainda, se for o caso, cobrada judicialmente. Acaso não tenha sido exigida garantia, à Administração se reserva o direito de descontar diretamente do pagamento devido à CONTRATADA o valor de qualquer multa porventura imposta.

Parágrafo quinto: Serão punidos com a pena de **SUSPENSÃO TEMPORÁRIA DO DIREITO DE CADASTRAR E LICITAR E IMPEDIMENTO DE CONTRATAR COM A ADMINISTRAÇÃO** aos que incorrerem nos ilícitos previstos nos incisos I, IV, VI e VII do art. 185 da Lei Estadual nº 9.433/05.

Parágrafo sexto: Serão punidos com a pena **de DECLARAÇÃO DE INIDONEIDADE PARA LICITAR E CONTRATAR COM A ADMINISTRAÇÃO**, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade competente para aplicar a punição, os que incorram nos ilícitos previstos nos incisos II, III e V do art. 185 da Lei Estadual nº 9.433/05.

Parágrafo sétimo: Para a aplicação das penalidades previstas serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato.

DA RESCISÃO

CLÁUSULA DÉCIMA SEGUNDA: O inadimplemento de cláusula estabelecida neste Contrato, por parte da CONTRATADA, assegurará ao CONTRATANTE o direito de rescindi-lo, mediante notificação, com prova de recebimento.

Parágrafo primeiro: A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento.

Parágrafo segundo: O CONTRATANTE ao longo da vigência do contrato poderá rescindi-lo conforme disposto no art. 168, da Lei nº 9.433/09, motivadamente, desde que seja a CONTRATADA notificada, por escrito, com antecedência de 30 (trinta) dias corridos, assegurados o contraditório e a ampla defesa.

Parágrafo terceiro: Quando a rescisão ocorrer com base nos incisos I e XVI a XX do art. 167, da Lei nº 9.433/09, sem que haja culpa da CONTRATADA, será esta ressarcida dos prejuízos regularmente comprovados que houver sofrido, tendo ainda direito a:

a) devolução da garantia;
b) pagamentos devidos pela execução do contrato até a data da rescisão;
c) pagamento do custo da desmobilização.

Parágrafo quarto: No caso de rescisão determinada por ato unilateral da CONTRATADA ficam asseguradas à CONTRATANTE, sem prejuízo das sanções cabíveis:

a) execução dos valores das multas e indenizações devidas à CONTRATANTE;
b) retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à CONTRATANTE.

Parágrafo quinto: O contrato poderá ser rescindido por acordo entre as partes, desde que haja conveniência para o CONTRATANTE, consoante o disposto no inciso II do art. 168 da Lei nº 9.433/05.

ACOMPANHAMENTO DOS PRAZOS DE GARANTIA E NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

CLÁUSULA DÉCIMA TERCEIRA: Durante a execução dos serviços deste Contrato, a CONTRATADA deverá prestar garantia e suporte, nos seguintes termos:

a) Considerando que a presente demanda se refere à contratação de Serviços com níveis predefinidos pelo fabricante, o Nível Mínimo de Serviço exigido para essa categoria de serviços será baseado no compromisso de qualidade e de prazos definidos no modelo "*Trend Micro™ Premium Support",* definida na Política de Suporte do fabricante da solução.

CLÁUSULA DÉCIMA QUARTA: Para o atendimento Níveis Mínimos de Serviço, a Contratada deverá atender ao quanto disposto no item 3.5. do Anexo I – Termo de Referência do Edital.

DA ALTERAÇÃO CONTRATUAL

CLÁUSULA DÉCIMA QUINTA – A CONTRATADA ficará obrigada a aceitar nas mesmas condições contratuais, acréscimos ou supressões que se fizerem no objeto, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma do §1º do art. 143 da Lei Estadual nº 9.433/05.

Parágrafo primeiro: Nenhum acréscimo ou supressão poderá ser realizado sem a devida motivação ou exceder o limite estabelecido no parágrafo anterior, salvo as supressões resultantes de acordo celebrado entre os contratantes.

DA REGÊNCIA LEGAL

CLÁUSULA DÉCIMA SEXTA - Submete-se, o presente contrato às disposições contidas na Lei Estadual nº 9.433/05 e suas alterações, Lei nº 12.846/2013, Lei 13.709/2018, Lei Complementar nº 123/2006, das Leis Federais nºs 10.520/02 e 8.666/93, , no que for pertinente, do Decreto Estadual nº 19.896/2020, Resolução nº 07/2005, alterada pela Resolução nº 229/16 do Conselho Nacional de Justiça, além dos Decretos Judiciários nº 12/03, 44/03, 13/06, 28/08 e 784/14 do TJBA, bem como aos demais dispositivos legais aplicáveis, obrigando a CONTRATADA a firmar todo e qualquer instrumento de retificação que tenha por objeto o cumprimento de prescrição legal e ou editalícia.

DA DOTAÇÃO ORÇAMENTÁRIA

CLÁUSULA DÉCIMA SÉTIMA - As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada:

Unidade Orçamentária	Unidade Gestora	Fonte	Projeto/Atividade	Elemento de despesa	SUB-ELEMENTO
02.04.601	0004-SETIM	113/120/320/ 313/326	2002/2034/2035/5051/ 5052/5054	3.3.90.40/ 4.4.90.52	40.02/40.06

No exercício subsequente, o respectivo orçamento consignará dotação própria para atender a despesa.

DO FORO

CLÁUSULA DÉCIMA OITAVA - As partes elegem o foro da Comarca de Salvador, Estado da Bahia para dirimir quaisquer dúvidas ou questões resultantes do cumprimento do presente contrato, com expressa renúncia de qualquer outro, por mais privilegiado que seja.

E, por estarem justas e Contratadas, as partes firmam o presente instrumento, em 3 (três) vias, de igual teor e forma, para um efeito, juntamente com as testemunhas, abaixo identificadas.

Salvador, ____ de _____ de 2023

CONTRATANTE	**CONTRATADA**
Testemunhas (nome CPF)	**Testemunhas (nome CPF)**

ANEXO AO CONTRATO - TERMO DE CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS
Lei n° 13.709/2018

ANEXO AO CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O ESTADO DA BAHIA, ATRAVÉS DO TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, E A EMPRESA XXXX, NA FORMA ABAIXO.

(Pregão Eletrônico nº XXXXXX Processo n° XXXXXXXXXXXXX)

O **ESTADO DA BAHIA**, pessoa jurídica de direito público, inscrito no CNPJ/MF sob o nº 13.937.032/0001-60, por intermédio do **TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA**, órgão do Poder Judiciário, inscrito no CNPJ/MF sob nº 13100722/0001-60, com sede e foro nesta cidade do Salvador, Estado da Bahia, na Quinta Avenida, nº 560, Centro Administrativo da Bahia – CAB, representado por **Des**. **NILSON SOARES CASTELO BRANCO** adiante denominada simplesmente **CONTRATANTE**, e, do outro lado, a empresa **XXXX** doravante designada simplesmente **CONTRATADA**, representada por XXXXXX resolvem, em conjunto, estabelecer regras para o cumprimento da Lei Geral de Proteção (Lei nº 13.709, de 14 de agosto de 2018), justando e reciprocamente aceitando as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste termo estabelece regras de tratamento e proteção de dados pessoais no Contrato n° XXX celebrado entre as partes acima descritas, adequando-o à Lei Geral de Proteção de Dados - LGPD (Lei n. 13.709, de 14 de agosto de 2018), na forma deste Anexo, parte integrante e indissociável.

CLÁUSULA SEGUNDA - CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

As partes se comprometem a manter sigilo e confidencialidade de todas as informações - em especial os dados pessoais e os dados pessoais sensíveis - repassadas em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

É vedada às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

Os dados pessoais devem ser armazenados pelo prazo necessário para cumprimento de legislação aplicável ao serviço, especialmente prevenção à lavagem de dinheiro.

As partes responderão administrativa e judicialmente caso causarem danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados.

A CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação, aplicando e aprimorando as medidas de prevenção e proteção à segurança dos dados que manuseia, com o intuito de proteger os dados pessoais repassados pelo CONTRATANTE.

A CONTRATADA fica obrigada a comunicar ao CONTRATANTE em até 24 (vinte e quatro) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

As partes têm conhecimento que as autorizações para tratamento de dados poderão ser revogadas, a qualquer momento, pela respectiva pessoa natural, mediante simples manifestação expressa, devendo as eventuais revogações de consentimento serem informadas uma a outra, a fim de que as devidas medidas sejam imediatamente adotadas.

A CONTRATANTE se compromete a cumprir toda legislação aplicável a segurança da informação, privacidade e proteção de dados, devendo adotar as medidas para, nos termos do art. 8º da LGPD, obter o consentimento prévio dos titulares para tratamento de seus dados, quando for o caso.

A CONTRATADA responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do CONTRATANTE, hipótese em que a CONTRATADA se equipara ao CONTRATANTE, salvo nos casos de exclusão previstos legalmente (art. 43 da Lei n. 13.709/2018).

CLÁUSULA TERCEIRA - DA PUBLICAÇÃO

Este Termo entrará em vigor a partir da publicação resumida do seu extrato no Diário da Justiça Eletrônico.

CLÁUSULA QUARTA – DO FORO

As partes elegem o foro da Comarca de Salvador-BA, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, as partes firmam o presente instrumento em 3 (três) vias de igual teor e um só efeito, juntamente com as testemunhas, abaixo identificadas.

Salvador, de de 2023.

TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA
Des. NILSON SOARES CASTELO BRANCO
Presidente do Tribunal de Justiça do Estado Bahia

XXXXXXXXXXXXXXX

Testemunhas:

_____	_____
Nome:	Nome:
CPF n°	CPF nº

ANEXO XIII - MODELO DE DECLARAÇÃO DE PROTEÇÃO AO TRABALHO DO MENOR

.....(nome da empresa), inscrita no CNPJ sob o nº ....., por intermédio do seu representante legal sr (a).....RG nº.....DECLARA, sob as penas da lei, em atendimento ao quanto previsto no inciso XXXIII do art. 7º da Constituição Federal, para os fins do disposto no inciso V do art. 98 da Lei Estadual 9.433/05, que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos.

Assinalar em caso afirmativo:

Emprega menor, a partir de 14 anos, na condição de aprendiz ( ).

Salvador, ...de .....de 2023.

_____

RAZÃO SOCIAL/ CNPJ/NOME DO REPRESENTANTE LEGAL/ E ASSINATURA

ANEXO XIV - MODELO DE DECLARAÇÃO DE NÃO INSCRIÇÃO DE EMPREGADOS FLAGRADOS EXPLORANDO TRABALHADORES.

PREGÃO Nº xxx/20xx Declaramos, sob as penas da Lei, que a empresa _____, inscrita no CNPJ sob o n. _____estabelecida na cidade de _____, Estado de _____, no endereço _____, telefone n° _____, por meio de seu representante, _____ _____, portador da Carteira de Identidade n._____, expedida pela _____, e do CPF n._____, para fins de participação na licitação, não possui inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pelo Ministério do Trabalho e emprego, por meio da portaria nº 540/2004. Por ser verdade, firmamos o presente.

Salvador, _____ de _____ de 2023

_____

RAZÃO SOCIAL, CNPJ, NOME DO REPRESENTANTE LEGAL E ASSINATURA

ANEXO XV - MODELO DE DECLARAÇÃO DE NÃO CONDENAÇÃO POR INFRINGIR AS LEIS DE COMBATE A DISCRIMINAÇÃO DE RAÇA OU DE GÊNERO.

PREGÃO Nº xxx/20xx Declaramos, sob as penas da Lei, que a empresa _____, inscrita no CNPJ sob o n. _____estabelecida na cidade de _____, Estado de _____, no endereço _____, telefone n° _____, por meio de seu representante, _____ _____, portador da Carteira de Identidade n._____, expedida pela _____, e do CPF n._____, para fins de participação na licitação, não foi condenada, a contratada ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta a previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal Brasileiro; do Decreto nº 5.017/2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nos 29 e 105. Por ser verdade, firmamos o presente.

Salvador, _____ de _____ de 2023.

_____

RAZÃO SOCIAL, CNPJ, NOME DO REPRESENTANTE LEGAL E ASSINATURA