**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# PROCESSO N° PRA-343/2024

# PREGÃO ELETRÔNICO Nº 27/2024

## PREÂMBULO

A Universidade de Taubaté – UNITAU, por intermédio do(a) Pregoeiro(a) especialmente designado pela Magnífica Reitora, torna público que realizará o PREGÃO ELETRÔNICO nº 27/2024, do **Tipo Menor Preço**, regido pela Lei Federal nº 14.133/21, Lei Complementar nº 123/06 e suas alterações e pelo Decreto Municipal de Taubaté n° 15.447/22.

## 1 - DO OBJETO E DA LICITAÇÃO

1.1. A presente licitação tem por objeto **Aquisição de solução de segurança corporativa para endpoints, servidores e rede UNITAU conforme especificações deste termo de referência, comtemplando suporte presencial/remoto para instalação, configuração, customização e treinamento, por 60 meses,** conforme condições estabelecidas neste instrumento convocatório e nos seguintes anexos: Anexo I – Modelo de Proposta Comercial, Anexo II – Declaração Unificada, Anexo III – Estudo Técnico Preliminar, Anexo IV – Mapa de Riscos, Anexo V – Termo de Referência e Anexo VI – Minuta de Contrato.

1.1.1. Critério de julgamento: **Menor Preço Unitário**.

1.1.2. Modo de disputa**: Modo aberto e fechado**.

1.1.3. Dotação orçamentaria**: As despesas decorrentes desse certame ocorrerão por conta da dotação** 12.122.4003.339030.

1.1.4. Valor estimado: **O valor estimado para a aquisição decorrente deste certame é de R R$ 469.660,00** (quatrocentos e sessenta e nove mil e seiscentos e sessenta reais).

1.1.5. **Início do recebimento das Propostas:** 22 de agosto de 2024.

1.1.6. **Fim do Recebimento das Propostas e documentos:** 14h30 de 04 de setembro de 2024.

1.1.7. **Abertura e avaliação das propostas:** 14h35 de 04 de setembro de 2024.

1.1.8. **Início da etapa de lances:** Após encerrada a abertura e avaliação das propostas e classificadas as propostas para a fase de lances, o pregoeiro abrirá, por comando próprio, a disputa.

1.1.9. **Referência de Tempo:** Horário de Brasília (DF).

1.1.10. **Local / Plataforma:** Compras BR – www.comprasbr.com.br.

## 2 - DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1. Poderão participar deste Pregão pessoas jurídicas constituídas e que satisfaçam integralmente a todas as exigências deste Edital e seus anexos.

2.2. É vedada a participação de:

2.2.1 Empresas impedidas de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo e empresas declaradas de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos.

2.2.2. Empresas enquadradas no art. 9, § 1° da Lei Federal nº 14.133/21.

2.2.3. Empresas em que participe, direta ou indiretamente, servidores ou dirigentes da Autarquia Municipal.

2.3. A participação neste Pregão implica o reconhecimento pela licitante de que conhece, atende e se submete a todas as condições do Presente Edital.

2.4. Para participação na licitação, a licitante deverá prover a sua inscrição e credenciamento através do Portal Compras BR - (www.comprasbr.com.br).

## 3 - DO CREDENCIAMENTO NO PORTAL COMPRAS BR

3.1. Para ter acesso ao sistema eletrônico, os interessados deverão dispor de chave de identificação e senha pessoal, obtidas junto ao provedor do sistema eletrônico (Compras BR), onde também deverão se informar a respeito do seu funcionamento e regulamento, obtendo instruções detalhadas para sua correta utilização.

3.2. Os interessados em se credenciar na plataforma Compras BR poderão obter maiores informações na página https://comprasbr.com.br/, podendo sanar eventuais dúvidas pela central de atendimentos da Plataforma ou pelo e-mail contato@comprasbr.com.br.

3.3. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

3.4. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ela efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou a Universidade de Taubaté responder por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros

3.5. O credenciamento junto à plataforma Compras BR implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a esta licitação.

3.6. A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso

3.7. A licitação será conduzida pelo Pregoeiro da Universidade de Taubaté, com apoio técnico e operacional da plataforma Compras BR, que atuará como provedor do sistema eletrônico para esta licitação.

## 4 - DA PROPOSTA DE PREÇOS

4.1. Após a divulgação do Edital no endereço eletrônico https://comprasbr.com.br/ e até a data e hora marcadas para abertura da sessão, os licitantes deverão encaminhar proposta com a descrição do objeto ofertado e preço, exclusivamente por meio do sistema eletrônico no endereço acima, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.

4.2. A Universidade de Taubaté não se responsabilizará por impossibilidade de inclusão, alteração ou exclusão de propostas por motivos de ordem técnica dos computadores, falhas de comunicação, congestionamento das linhas de comunicação, bem como outros fatores que impossibilitem a transferência de dados.

4.2.1. No campo apropriado do sistema eletrônico, será **obrigatório** preencher a coluna marca.

4.2.2. Para que não haja identificação, caso a empresa seja a **fabricante do produto**, no campo marca e modelo deverá ser escrito **PRÓPRIA**, não identificando o nome da empresa.

4.3. A licitante deverá elaborar a sua proposta com base no edital e seus anexos, sendo de sua exclusiva responsabilidade o levantamento de custos necessários para o cumprimento total das obrigações necessárias para a execução do objeto desta licitação. Até a abertura da sessão, os licitantes poderão retirar ou substituir as propostas apresentadas.

4.4. O licitante deverá enviar sua proposta, no idioma oficial do Brasil, mediante o preenchimento, no sistema eletrônico, do valor unitário e total, em moeda corrente nacional com 02 (duas) casas decimais após a vírgula;

4.5. Todas as especificações do objeto contidas na proposta vinculam a Contratada e, havendo divergência entre as condições da proposta e as cláusulas deste Edital, incluindo seus anexos, prevalecerão as últimas.

4.6. No(s) preço(s) cotado(s) deverão estar embutidos todos os custos diretos e indiretos, despesas indiretas (BDI), transportes, carga e descarga, seguro, impostos, taxas, multas, emolumentos legais, custos de mobilização de equipamentos e pessoas, além de transporte, estada e alimentação da equipe de trabalho, insumos e demais encargos, inclusive previdenciários e trabalhistas, seguro de qualquer espécie, licenças, documentos e despesas, tributos inclusive ICMS ou ISSQN se houver incidência, encargos e incidências diretos e indiretos, que possam vir a gravá-los e lucro, sendo de inteira responsabilidade da empresa proponente a quitação destes, que em momento algum e sob nenhuma alegação, inclusive falta de previsão oficial, poderão ser transferidos à Universidade de Taubaté, a responsabilidade de seus pagamentos, quitação ou outras quaisquer decorrentes.

4.7. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do Licitante.

4.8. Não poderá ser ofertada quantidade inferior ao solicitado em edital.

4.9. O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

4.10. Declarações falsas, relativas ao cumprimento dos requisitos, sujeitarão a licitante às sanções previstas na Lei Federal 14.133/21.

## 5 - DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á mediante comando do pregoeiro, por meio de sistema eletrônico, na data e horário indicados no preâmbulo deste edital.

5.2. Durante a sessão pública, a comunicação entre o pregoeiro e os licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema.

5.3. O pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos no Edital, que contenham vícios insanáveis ou não apresentem especificações técnicas exigidas no Edital e seus anexos.

5.4. A proposta que, de alguma forma, identifique o licitante também será desclassificada.

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

5.6. A não desclassificação da proposta não implica em sua aceitação definitiva, que deverá ser levada a efeito após seu julgamento definitivo.

5.7. Após, o sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

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

5.9. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.10. Em caso de falha no sistema, os lances em desacordo com a norma deverão ser desconsiderados pelo Pregoeiro, devendo a ocorrência ser comunicada imediatamente ao provedor do sistema eletrônico (Compras BR).

5.11. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.
5.12. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.13. Durante o transcurso da sessão, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.13. Será adotado o modo de disputa “aberto e fechado”, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.14. A etapa de lances da sessão terá duração inicial de 15 (quinze) minutos e, após esse prazo, o sistema encaminhará o aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até 10 (dez) minutos, aleatoriamente determinado, findo qual será automaticamente encerrada a recepção de lances.

5.15. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e o das ofertas com preço de até 10% (dez por cento) superiores aquela possam ofertar lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

5.15.1. Não havendo pelo menos 03 (três) ofertas nas condições estabelecidas no subitem 5.15, poderão os autores dos melhores lances, na ordem de classificação, até o máximo de 03 (três), oferecer um lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

## 6 - DA ACEITABILIDADE E ENCAMINHAMENTO DA PROPOSTA VENCEDORA

6.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar, quanto a adequação ao objeto e a compatibilidade do preço em relação ao máximo estimado pelo órgão.

6.2. Será desclassificada a proposta ou lance vencedor que apresentar preço final superior ao valor máximo estimado pelo órgão, ou que apresentar preço inexequível.

6.2.1. Considera-se valor inexequível a proposta que apresente preços simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado.

6.2.2. Qualquer interessado poderá requerer que se realize diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentem a suspeita.

6.3. Na hipótese de necessidade de suspensão da sessão pública para realização de diligências, o pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

6.4. Encerrada a etapa de aceitação da proposta, o pregoeiro verificará a habilitação do licitante autor da melhor proposta, observando o disposto em edital.

## 7 - DA HABILITAÇÃO

7.1. Para fins de habilitação, as licitantes deverão encaminhar via Plataforma do Compras BR, preferencialmente após o término da etapa de Lances, os seguintes os documentos.

7.1.1. Caso a Licitante opte por anexar toda a Documentação de Habilitação concomitantemente ao cadastro da proposta na plataforma, não haverá nenhum prejuízo à mesma. O pregoeiro concederá ainda o prazo de 01 (uma) hora, após o término da etapa de Lances, para que a mesma insira a documentação.

7.1.2. Caso a Licitante comunique via Chat que concluiu a inserção dos Documentos, o prazo de 01 (uma) hora será findado, e o Pregoeiro iniciará a análise dos mesmos, sendo vedada a inserção de novos documentos a partir desde momento, salvo nos casos de diligência.

7.2. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto a existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta de Cadastro de impedidos de licitar do TCE/SP e consulta consolidada de pessoa Jurídica do Tribunal de Contas da União.

7.2.1. Contatada a existência de sanção, o pregoeiro inabilitará o licitante, por falta de condição de participação.

**7.3. Habilitação Jurídica**

7.3.1. Registro Comercial, no caso de empresa individual.

7.3.2. Ato Constitutivo, Estatuto ou Contrato Social em vigor, e alterações posteriores, ou consolidado, devidamente registrado no órgão competente, em se tratando de sociedade comercial; no caso de sociedade por ações, acompanhada de documento de eleição de seus administradores e, no caso de sociedade civil, acompanhada da Inscrição do Ato Constitutivo e de prova da diretoria em exercício.

7.3.3. Em se tratando de empresa ou sociedade estrangeira em funcionamento no País, deverá ser apresentado decreto de autorização e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

**7.4. Regularidade Fiscal e Trabalhista**

7.4.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ.

7.4.2. Certidão Conjunta de Débitos relativos a Tributos Federais e a Dívida da União, emitida pela Receita Federal do Brasil (RFB) e Procuradoria-Geral da Fazenda Nacional (PGFN).

7.4.3. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), por meio de Certificado de Regularidade, emitido pela Caixa Econômica Federal.

7.4.4. Certidão Negativa de Débitos Tributários, expedida pelo órgão fazendário estadual da sede do licitante, ou declaração de isenção ou de não incidência, assinada pelo (s) representante (s) legal (is) da empresa, sob as penas da lei.

7.4.5. Certidão Negativa de Débitos Tributários Mobiliários - Imposto sobre Serviços de Qualquer Natureza (ISSQN), expedida pelo órgão fazendário municipal, ou declaração de isenção ou de não incidência, assinada pelo(s) representante(s) legal (is) da empresa, sob as penas da lei.

7.4.6. Certidão Negativa de Débitos Trabalhistas (CNDT), nos termos da Lei nº 12.440, de 07 de julho de 2011.

**7.5. Qualificação econômico-financeira**

7.5.1. Certidão negativa de falência, em se tratando de sociedade comercial, ou certidão negativa de execução patrimonial, em se tratando de sociedade civil, expedida pelo distribuidor da sede da pessoa jurídica e, em se tratando de pessoa física, expedida no domicílio da pessoa física, datada de, no máximo, 90 (noventa) dias anteriores à abertura desta sessão.

**7.6. Qualificação Técnica**

7.6.1. Atestado(s) emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, em nome do licitante, em pelo menos 50% da quantidade do Objeto. O(s) atestado(s) deverá(ão) conter: prazo contratual e datas de início e término; local da prestação dos serviços; natureza da prestação dos serviços; quantidades executadas; caracterização do bom desempenho do licitante; outros dados característicos; e a identificação da pessoa jurídica emitente bem como o nome e o cargo do signatário.

7.6.2 A referida comprovação poderá ser efetuada pelo somatório das quantidades realizadas em tantos contratos quanto dispuser o licitante.
7.6.3 O(s) documento(s) deve conter a razão social, CNPJ, o nome e assinatura do representante legal, o endereço e o telefone de contato do(s) atestado(res), ou qualquer outra forma de que a Universidade de Taubaté possa valer-se para manter contato com a(s) empresa(s) declarante(s).
7.6.4 O Atestado de Capacidade Técnica deverá comprovar o fornecimento, instalação, treinamento, manutenção e suporte na solução ofertada.

**7.7. Das Declarações**

7.7.1. Declaração unificada, conforme modelo Anexo II do Edital.

7.8. O pregoeiro poderá realizar a atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

7.8.1. No caso acima, a verificação pelo Pregoeiro em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.8.2. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

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

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

7.9. Todas as certidões, declarações ou documentos equivalentes expedidos sem prazo de validade serão considerados válidos, desde que expedidos a no máximo 180 (cento e oitenta) dias anteriores à data designada para a abertura da sessão pública.

7.10. Caso a licitante declarada vencedora seja enquadrada como ME ou EPP, deverá remeter toda Documentação de comprovação fiscal e trabalhista, mesmo que esta apresente alguma restrição.

7.10.1. Havendo alguma restrição, a mesma terá 05 (cinco) dias úteis, prorrogados por igual período a critério da Administração Pública, para regularizar pendências FISCAIS ou TRABALHISTAS, conforme o disposto nos artigos 42 e 43 da Lei Complementar nº 123/2006 e suas alterações, a contar da publicação de homologação da Licitação.

7.10.2. Caso a Microempresa ou Empresa de Pequeno Porte que se beneficiar no disposto no subitem 8.6.6.1. não o fizer dentro do prazo estipulado no mesmo subitem, implicará a decadência do direito a contratação, procedendo-se a convocação dos licitantes remanescentes.

7.11. Havendo necessidade de analisar minuciosamente os documentos exigidos, o pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

7.12. É facultado ao pregoeiro, auxiliado pela Equipe de Apoio, proceder em qualquer fase da licitação diligências destinada a esclarecer ou complementar a instrução do processo julgadas necessárias à análise das propostas e da documentação, devendo os licitantes atender as solicitações no prazo por ele estipulado, contado do recebimento da convocação.

## 8 - DOS RECURSOS

8.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como micro empresa e empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo 10 (dez) minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, em campo próprio no sistema.

8.1.1. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito, ficando o pregoeiro autorizado a prosseguir o certame e declarar a vencedora.

8.2. Havendo quem se manifeste, caberá ao pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

8.3. Nesse momento o pregoeiro não adentrará ao mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

8.4. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de 03 (três) dias úteis para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros 03 (três) dias úteis, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.5. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.6. As razões e contrarrazões serão recebidas exclusivamente por meio de campo próprio no Sistema Compras BR.

8.7. Caberá ao pregoeiro receber, examinar e instruir os recursos interpostos contra seus atos, podendo reconsiderar suas decisões ou, fazê-lo subir, devidamente informado à autoridade superior ao Pregoeiro, com competência para decidir recursos, para a decisão final.

8.8. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento

8.9. Não serão conhecidos os recursos apresentados fora dos prazos, subscritos por representantes não habilitados legalmente ou não identificados no processo para responder pelo licitante.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

## 9 - DA REABERTURA DA SESSÃO PÚBLICA

9.1. A sessão pública poderá ser reaberta nas seguintes hipóteses:

9.1.1. Em caso de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

9.1.2. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o Contrato ou a Ata de Registro de Preços, outro licitante poderá ser convocado, respeitada a ordem de classificação, para, após a comprovação dos requisitos de habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o Contrato ou a Ata de Registro de Preços.

9.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

9.2.1. A convocação se dará por meio do sistema eletrônico (“chat”).

## 10 - DA ADJUDICAÇÃO E HOMOLOGAÇÃO

10.1. Após a fase recursal, se for o caso, constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto da licitação ao(s) licitante(s) declarado(s) vencedor(es).

10.2. A vencedora deverá encaminhar a proposta realinhada de todos os itens vencidos através do e-mail questionamentos@unitau.br ou da plataforma Compras BR.

10.2.1. A proposta realinhada deverá seguir o modelo do Anexo I do edital.

10.3. Após o envio dos documentos referentes ao subitem 10.2., a autoridade competente homologará o procedimento licitatório.

## 11 - DA CONTRATAÇÃO

11.1. A contratação decorrente desta licitação será formalizada mediante a celebração de termo de contrato, cuja minuta integra este edital como Anexo VI, e não poderá ser objeto de subcontratação.

11.2. A adjudicatária deverá assinar o contrato relativo ao objeto adjudicado, no prazo de 05 (cinco) dias úteis, **a contar da Homologação do Objeto**.

11.2.1. Caso a empresa tenha apresentado alguma restrição fiscal e/ou trabalhista, a adjudicatária deverá assinar o contrato, no prazo de 05 (cinco) dias úteis, a contar da regularização constante no item 7.9.1. do edital.

11.2.2. A recusa injustificada da licitante vencedora em assinar o Contrato, caracterizará o descumprimento da obrigação assumida, considerando-se decaído seu direito de vencedor e sujeitando-o à seguinte penalidade:

a) multa de 30% trinta por cento), sobre o valor total homologado.

b) a multa deverá ser recolhida, por depósito bancário identificado, na conta corrente nº 45.000045-5, agência 0056, Banco Santander, em nome da Universidade de Taubaté, no prazo de até 05 (cinco) dias, a contar do recebimento da notificação do setor responsável.

c) o comprovante de depósito deverá ser encaminhado, no prazo acima, ao e-mail do setor responsável pela notificação.

d) para a penalidade prevista, será garantido o direito ao contraditório e à ampla defesa, que será dirigida para análise da Douta Procuradoria Jurídica.

e) a penalidade só poderá ser relevada nas hipóteses de caso fortuito ou força maior, devidamente justificada e comprovada, a juízo da Administração.

11.3. É facultado à UNITAU, na hipótese de recusa da licitante vencedora em assinar o contrato, convocar para contratação outro licitante, respeitada a ordem de classificação, na forma dos subitens 9.2 e 9.2.1.

11.3.1. Não serão apenadas as licitantes convocadas na forma do subitem 11.3. supra que não concordarem em celebrar o contrato.

11.4. O prazo de vigência deste instrumento será conforme Anexo VI – Minuta de Contrato.

11.4.1. É facultado à UNITAU, na hipótese de recusa da licitante vencedora em assinar o contrato, convocar para contratação outro licitante, respeitada a ordem de classificação, na forma dos subitens 9.2 e 9.2.1.

11.4.2. Não serão apenadas as licitantes convocadas na forma do subitem 11.4.1. supra que não concordarem em celebrar o contrato.

## 12 - DAS COMINAÇÕES

12.1. Pela inexecução total ou parcial do objeto contratado, deixar de entregar documentação exigida, não manter a proposta, erro de execução, execução imperfeita, retardamento da execução ou da entrega do objeto, inadimplemento contratual ou ainda comportar-se de modo inidôneo, cometer fraude de qualquer natureza ou constatar-se a não veracidade de informações prestadas à Administração, praticar atos ilícitos e lesivos, poderá a Administração aplicar a Licitante ou a Contratada, garantida a prévia e ampla

defesa, nos termos do Art. 155, da Lei Federal nº 14.133/21, as sanções administrativas que seguem:

a) advertência por escrito por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos ao objeto contratado, sendo exigida pronta reparação da falta cometida e comunicação formal das providências tomadas;

b) multa de 2% (dois por cento), sobre o valor total do contrato, por reincidência de 02 (duas) advertências;

c) multa equivalente a 4% (quatro por cento), sobre o valor total do contrato, por dia, pelo não cumprimento dos prazos de entrega, admitindo-se o máximo de 05 (cinco) dias, após o que poderá ser reconhecida a inexecução do ajuste;

d) multa de 10% (dez por cento), sobre o valor total do contrato, por infração a qualquer condição do contrato e, aplicada em dobro, em caso de reincidência;

e) multa de 20% (vinte por cento), sobre o valor total do contrato, por inexecução parcial deste ajuste, observando-se a proporcionalidade de parte do contrato cumprido, independentemente das demais sanções cabíveis;

f) multa de 30% (trinta por cento), sobre o valor total do contrato, por inexecução total deste juste, independentemente das demais sanções cabíveis;

g) multa de 30% (trinta por cento), sobre o valor total homologado, pela recusa injustificada da licitante vencedora em assinar o Contrato;

h) no caso de reincidência em irregularidades na execução do objeto por 03 (três) vezes, poderá considerar caracterizada a inexecução do objeto e rescindir o ajuste, sem prejuízo das multas estipuladas nas alíneas anteriores;

i) impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo, por prazo de 03 (três) anos, nos casos descritos nos incisos III, IV, V e VI do caput do art. 155 da Lei Federal 14.133/2021, e por prazo de 02 (dois)

anos, nos casos descritos nos incisos II, VII do caput do art. 155, da Lei Federal 14.133/2021, admitindo-se a sua reabilitação nos termos do Art. 163, da mesma lei.

j) declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, por prazo de 06 (seis) anos, nos casos descritos nos incisos VIII, IX, X, XI e XII do caput do art. 155 da Lei Federal 14.133/2021, admitindo-se a sua reabilitação nos termos do Art. 163, da mesma lei.

12.2. As multas deverão ser recolhidas, por depósito bancário identificado, na conta corrente nº 45.000045-5, agência 0056, Banco Santander, em nome da Universidade de Taubaté, no prazo de até 15 (quinze) dias úteis, contado da data de sua intimação.

12.2.1. O comprovante de depósito deverá ser encaminhado, no prazo acima, ao e-mail do setor responsável pela intimação.

12.3. Se o valor da multa aplicada e as indenizações cabíveis não forem pagos, os mesmos deverão ser descontados dos pagamentos eventualmente devidos à Administração, ou descontados da garantia prestada ou será cobrada judicialmente.

12.4. A aplicação das penalidades não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

12.5. Para as penalidades previstas, será garantido o direito ao contraditório e à ampla defesa, a qual deverá ser apresentada pelo interessado no prazo de 15 (quinze) dias úteis, contado da data de sua notificação, que será dirigida para análise da Douta Procuradoria Jurídica;

12.6. As sanções serão obrigatoriamente registradas em autos próprios, e no caso da aplicação do impedimento de licitar e contratar e da declaração de inidoneidade, requererá a instauração de processo de responsabilização, a ser conduzido por comissão, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação,

apresentar defesa escrita e especificar as provas que pretenda produzir, nos termos do Art. 158, da Lei Federal 14.133/21.

12.7. As penalidades só poderão ser relevadas nas hipóteses de caso fortuito ou força maior, devidamente justificada e comprovada, a juízo da Administração.

## 13 - DA EXECUÇÃO

13.1. A execução do objeto ocorrerá conforme disposto no Anexo V (Termo de Referência).

## 14 - DO PAGAMENTO

14.1. O pagamento será realizado conforme disposto no Anexo V (Termo de Referência).

14.2. O pagamento será efetuado observado as seguintes condições:

14.2.1. Apresentação de nota fiscal/fatura.

14.2.2. Em atenção à Instrução Normativa RFB nº 2145, de 26/06/2023, informamos que é **obrigatório** destacar o valor e a alíquota do IR a ser retido **no corpo da Nota Fiscal**. Caso o fornecedor seja isento ou imune, uma declaração deverá ser apresentada.

14.3. Notas Fiscais emitidas em “não conformidade” com as exigências da Unitau deverão ser canceladas pela contratada.

14.4. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a correção monetária.

14.5. Não será admitida a transferência de obrigações a terceiros (empresas de fomento, etc.), devendo o pagamento ser realizado única e exclusivamente à licitante vencedor.

## 15 - DA IMPUGNAÇÃO DO EDITAL E DO PEDIDO DE ESCLARECIMENTO

15.1. Até 03 (três) dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa, física ou jurídica, poderá solicitar esclarecimentos ou impugnar este Edital de Pregão.

15.1.1. O documento de esclarecimento e impugnação deverá ser feito por forma eletrônica, via plataforma www.comprasbr.com.br

15.2. Serão respondidos os pedidos de esclarecimentos por meio do sistema eletrônico, no prazo de 03 (três) dias úteis, contados da data de recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame e quanto a impugnação, será decidida e respondida pelo mesmo meio, via sistema, no prazo de até 03 (três) dias úteis, contados da data de recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame, sendo que caso não seja possível resolver a impugnação contra o Edital, será definida e publicada nova data para a realização do certame

15.3. Caso acolhida a impugnação contra o Edital, será designada nova data para a realização do certame, dando conhecimento aos interessados.

15.4. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

## 16 - DAS DISPOSIÇÕES GERAIS

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

16.2. O resultado da sessão pública deste certame será divulgado em Ata no sistema eletrônico da www.comprasbr.com.br. e no portal da Universidade de Taubaté no sítio www.unitau.br/licitacoes.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

16.3. A Universidade poderá ampliar ou reduzir em até 25% (vinte e cinco por cento) a quantidade do material ou serviço a ser fornecido dentro dos termos deste edital e o vencedor se obriga ao fornecimento.

**Universidade de Taubaté**

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# ANEXO I

## MODELO DE PROPOSTA COMERCIAL

(Licitante vencedor)

**À**
**UNIVERSIDADE DE TAUBATÉ**
**Ref.: PREGÃO ELETRÔNICO Nº 27/2024**
**Processo PRA-343/2024**

Apresentamos nossa proposta de preço, em 01 (uma) via, para **Aquisição de solução de segurança corporativa para endpoints, servidores e rede UNITAU conforme especificações deste termo de referência, comtemplando suporte presencial/remoto para instalação, configuração, customização e treinamento, por 60 meses**, conforme especificações constantes do Anexo V, que integra o presente EDITAL, consistindo no seguinte:

| Item | Descrição | Qtde. | Unidade de Medida | Valor Unitário (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| **01** | SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, CONFORME ESPECIFICAÇÕES ANEXAS. | 2.000 | LICENÇA | | |

**I)** O prazo de validade de nossa proposta é de no mínimo 60 (sessenta) dias, a contar da data da sessão pública do pregão.

**II)** O prazo de execução será de _____ (_____) dias, contado a partir do 1º dia útil subsequente a assinatura do Contrato, conforme Termo de Referência (Anexo V) e Minuta de Contrato (Anexo VI).

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**III)** O prazo de pagamento será de até _____ (____) dias após o ateste da Nota Fiscal pelo responsável, conforme constante no Termo de Referência (Anexo V) e Minuta de Contrato (Anexo VI).

**IV)** Declaramos que no preço apresentado estão ainda inclusos:

**a -** os valores dos materiais, matérias-primas, mão-de-obra, treinamento básico operacional, frete, transporte e equipamentos e afins fornecidos, acrescidos de todos os respectivos encargos sociais;
**b -** taxa de administração, emolumentos, quaisquer despesas operacionais e outros encargos;
**c -** todos os tributos, encargos trabalhistas, previdenciários, fiscais e comerciais, prêmios de seguro, bem como demais encargos, se exigidos na forma da lei, tais como: horas extras e adicionais noturnos de profissionais, auxílio-alimentação, transporte, inclusive sob a forma de auxílio-transporte, transporte local, etc.;
**d -** despesas e obrigações financeiras de qualquer natureza;
**e -** quaisquer outras despesas, diretas ou indiretas, enfim, todos os componentes de custo dos produtos, necessários à perfeita satisfação do objeto deste Edital, até o Recebimento Definitivo, inclusive o prazo de garantia, de acordo com o estabelecido no Edital.

**V)** Declaramos ainda conhecer integralmente os termos do presente Edital e seus respectivos Anexos, aos quais nos sujeitamos.

**VI)** Dados da empresa:
CNPJ empresa nº ...../.....-.....Inscrição Estadual nº.....Estado .....Inscrição Municipal nº.....Município.....Endereço.....
.....CEP.....Telefone.....
.....Fax..... nº da conta corrente.....Banco.....Agência.....Praça ..... para fins de pagamento.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**VII)** Dados do representante legal pela assinatura do contrato:

Nome completo:_____

RG _____ CPF/MF_____

E-mail comercial _____ E-mail pessoal _____

função na empresa_____

....., ..... de ..... de 2024.

---

(Nome Legível)

**OBSERVAÇÕES**

**1) Esta Proposta Comercial realinhada (Anexo I) deverá ser preenchida pela licitante vencedora, com o carimbo da licitante e em papel timbrado da empresa no formato deste Anexo I.**

**2) Necessariamente todos os itens constantes neste MODELO deverão estar presente na Proposta Comercial apresentada.**

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# ANEXO II

## MODELO DE DECLARAÇÃO UNIFICADA

A empresa_____sediada na Rua (Av., Al., etc.)_____, cidade _____, estado ___, inscrita noCNPJ sob nº_____, por seu diretor (sócio gerente, proprietário)_____, portador(a) da Carteirade Identidade nº____ _____, e inscrito(a) no CPF/MF com o nº_____, **DECLARA**, sob as penas da Lei, que:

1. Até a presente data inexiste fato impeditivo para sua habilitação NO PREGÃO ELETRÔNICO n° ____/2024, ora sendo realizada pela Universidade de Taubaté, comprometendo-se a comunicar a eventual ocorrência desses fatos durante o processamento desta contratação.

2. Para fins de participação neste pregão eletrônico, ora sendo realizada pela Universidade de Taubaté, que preenche todos os requisitos de habilitação previstos neste edital.

3. Se enquadra na situação de ME - Microempresa ou de EPP - Empresa de Pequeno Porte, nos termos da legislação vigente e bem assim que inexistem fatos supervenientes que conduzam ao seu desenquadramento desta situação. Em sendo ME/EPP declara ainda não ter celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de Porte, em observância ao Art. 4° da Lei Federal 14.133/21.

4. Não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos. Cumpro as exigências de reserva de cargos para pessoas com deficiência e para reabilitados da Previdência Social e para aprendiz, previstas em lei e em outras normas específicas.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

5. Não possuir em seu quadro societário Servidor Público deste órgão.

Sr.(a). _____, cargo _____, portador da certeira de identidade n° _____ e CPF _____ representante legal da empresa _____, CNPJ _____, assinará a ATA/Contrato ou receberá a autorização de compra.

E-mail Pessoal: _____

E-mail Profissional: _____

_____, ____ de _____ de 20____.

**Nome e Assinatura do representante da empresa.**

**Obs: ESTA DECLARAÇÃO DEVERÁ SER PREENCHIDA EM PAPEL TIMBRADO DA EMPRESA E ASSINADA PELO(S) SEU(S) REPRESENTANTE(S) LEGAL(IS) E/OU PROCURADOR(ES) DEVIDAMENTE HABILITADO(S).**

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# ANEXO III

## ETP
## ESTUDO TÉCNICO PRELIMINAR
## ETP CETI Nº 010/2024

### 1 Descrição da necessidade

Na tecnologia de informação e comunicação (TIC) as ameaças à segurança têm crescido de forma galopante nos últimos anos. Hoje são necessárias várias camadas de proteção tanto na rede, servidores, e-mails, computadores e até smartphones.

A solução que pretendemos adquirir deve completar de forma mais justa e eficiente as outras camadas que já dispomos de segurança e as que planejamos adquirir.

Nos ataques mundiais de ransomware ocorridos ultimamente ficou clara a necessidade de backup, proteção dos endpoints e atualização dos sistemas operacionais (de uma forma bastante resumida).

Outras soluções poderão superpor medidas já utilizadas ou deixar outras sem nenhuma cobertura.

Portanto, uma solução de segurança complementar às já existentes. Não devendo duplicar funções já existentes, mas cobrir as áreas ainda não contempladas pelas outras camadas de soluções.

É fundamental manter recursos tecnológicos que garantam a segurança dos dados e informações de propriedade ou sob custódia das áreas de negócio da UNITAU, haja vista a necessidade fundamental de proteção dos dados, de grande valor para a instituição, contra os mais diversos tipos de ameaças.

**A CONTRATAÇÃO ATUAL TERÁ SEU VENCIMENTO EM 22/11/2024, PORTANTO O NOVO CONTRATO DEVERÁ INICIAR A PARTIR DE 23/11/2024.**

### 2 Demonstrando o Alinhamento da aquisição/contratação e o planejamento

A aquisição do serviço descrito no presente Estudo foi devidamente prevista e aprovada no PAC 2024, e consta no PCA – Plano de Contratação Anual.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

## 3 Requisitos da aquisição/contratação

As empresas licitantes deverão informar claramente na Proposta a marca e modelo da solução, sob pena de desclassificação.

Contratação do serviço conforme abaixo:

| Item | Descrição | UNID |
|---|---|---|
| **01** | SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, CONFORME ESPECIFICAÇÕES ANEXAS. | **LICENÇA** |

Solução de segurança corporativa para endpoints, conforme especificações do termo de referência, inclui suporte presencial/remoto para instalação, configuração, customização e eventuais treinamentos que se fizerem necessários ao longo dos 60 meses.

Aquisição de software de proteção antivírus, com funcionalidades antispyware, de controle de dispositivos, de prevenção de intrusos (IPS) e firewall para rede, estações de trabalho e servidores de arquivos/aplicações da UNITAU, sendo máquinas físicas ou virtuais e em ambiente local ou em nuvem, incluindo: instalação e configuração dos softwares da solução, incluindo desinstalações de softwares anteriores, se for o caso; Operação assistida de funcionamento da solução; atualização de software e base de assinaturas; treinamento presencial ou on-line, em português, com interação entre as partes, para 6 (seis) servidores da UNITAU e treinamentos contínuos online em plataforma web própria tanto da solução adquirida, quanto das demais soluções para ampliação de conhecimentos técnicos; os treinamentos serão aceitos de forma on-line desde que a Contratada, ofereça ferramentas e ambientes para simulação e configuração conforme a estrutura verificada no momento da instalação na UNITAU. Além disso, os treinamentos e/ou reuniões on-line deverão ser gravados e disponibilizados para consultas posteriores; e suporte técnico pelo período de 60 (sessenta) meses, conforme especificações deste Estudo Técnico Preliminar.

### 3.1 Console de gerenciamento centralizado

**3.1.1** O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor.

**3.1.2** O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS) compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.

**3.1.3** O acesso ao Console deve suportar várias sessões simultâneas.

**3.1.4** Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.

**3.1.5** Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor.

**3.1.6** Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.

**3.1.7** O **servidor de gerenciamento** deve possuir compatibilidade para instalação nos seguintes sistemas operacionais, **de 64 bits ou 32 bits, quando existentes, e versões posteriores, inclusive nas que foram lançadas durante a vigência do contrato,** bem como em todas as versões/distribuições/releases e Hypervisors:

**a)** Microsoft Windows 7;

**b)** Microsoft Windows Server 2012 e R2;

**c)** Microsoft Windows Server 2016 (Server Core e Desktop Experience);

**d)** Ubuntu 18.04.1 LTS Desktop e Server;

**e)** Red Hat Enterprise Linux 7;

**f)** CentOS 7;

**g)** Debian 10;

**h)** VMware vSphere/ESXi 6.5;

**i)** VMware Workstation 9;

**j)** VMware Player 7;

**k)** Microsoft Hyper-V Server 2012;

**l)** Oracle VirtualBox 6.0;

**m)** Citrix 7.0 e posterior.

**3.1.8** O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE, ou seja, será instalado completamente no ambiente da UNITAU e também ter a opção de gerenciamento em nuvem, pois temos máquinas em redes internas sem acesso a Internet e também com acesso a Internet e sem acesso a rede interna.

**3.1.9** O console de gerenciamento deve oferecer também, opção para gerenciamento em nuvem, disponibilizado pela CONTRATADA.

**3.1.10** Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.

**3.1.11** Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.

**3.1.12** Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.

**3.1.13** Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso).

**3.1.14** Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.

**3.1.15** Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.

**3.1.16** Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

**3.1.17** O console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.

**3.1.18** Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador).

**3.1.19** A solução deve possuir sistema RBAC (Role Based Access Control) para definir acessos customizados de usuários adicionais no console, oferecendo granularidade para configuração dos acessos, para segregar os acessos, limitando os acessos a não exclusivamente políticas, tarefas, e demais objetos do console.

**3.1.20** O log deve ser centralizado e conter, no mínimo, os seguintes itens:

**a)** Nome da ameaça;

**b)** Nome do arquivo infectado;

**c)** Caminho da detecção;

**d)** HASH do arquivo;

**e)** Data e hora da infecção;

**f)** Ação tomada;

**g)** Endereço de IP da máquina;

**h)** Usuário autenticado na máquina;

**i)** Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado;

**3.1.21** Fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações:

**a)** Nome da máquina;

**b)** Endereço IP da máquina;

**c)** Malwares não removidos;

**d)** Status da conexão;

**e)** Data da vacina;

**f)** Versão do antivírus instalado.

**3.1.22** O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques. Suportando no mínimo alertas dos seguintes módulos:

**a)** Detecções de Malware;

**b)** Detecções de Firewall;

**c)** Detecções via EDR;

**3.1.23** Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.

**3.1.24** Capacidade de voltar (rollback) para versão de atualização (da solução ou vacina) através de procedimento específico no console de gerenciamento.

**3.1.25** Interface da Console de Gerenciamento totalmente em português.

**3.1.26** Deve permitir criar o backup da Base de dados da Console de gerenciamento.

**3.1.27** O acesso a console de gerenciamento deverá ser autenticado.

**3.1.28** A console deverá funcionar também através de um Appliance Virtual fornecido pelo fabricante.

**3.1.29** O acesso ao console de administração do antivírus deve permitir a possibilidade de ser feito com duplo fator de autenticação integrado dentro da mesma console onde é possível ativá-lo sem a necessidade de nenhum add-on adicional.

**3.1.30** Gerar pacotes de instalação dos clientes, para cada tipo de sistema operacional existente na estrutura da CONTRATANTE, possibilitando a gravação em mídia e a instalação do software em ambientes onde não seja possível a instalação via rede corporativa.

**3.1.31** Permitir forçar a instalação do software cliente do antivírus nos computadores, reinstalando-o em caso de desinstalação ou corrupção do mesmo.

**3.1.32** Atualização de vacinas sem a necessidade de reinicialização.

**3.1.33** Suportar o gerenciamento de todos os clientes instalados nas máquinas (estações de trabalho, servidores, tablets e smartphones) a partir do servidor de Console de Gerenciamento, oferecendo a possibilidade de configuração centralizada e remota de todas as funcionalidades.

**3.1.34** Gerenciar de forma remota as configurações do firewall local de cada máquina com o cliente instalado.

**3.1.35** A solução deve oferecer recurso para isolar as máquinas da rede, mantendo apenas comunicação segura com o servidor de gerenciamento.

**3.1.36** Criação de grupos e subgrupos de máquinas baseada na hierarquia do Active Directory e LDAP ou em identificador único de clientes, tal como endereço IP;

**3.1.37** Forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada na console de gerenciamento.

**3.1.38** Atualização/sincronização de configurações nos clientes sem a necessidade de reinicialização ou logoff.

**3.1.39** Permitir a criação de tarefas de rastreamento em períodos de tempo pré-determinados e na inicialização do sistema operacional.

**3.1.40** Permitir a criação de tarefas de atualização de vacinas e novas versões de software em períodos de tempo pré-determinados.

**3.1.41** Permitir o uso de ferramentas para centralizar a distribuição de atualizações de software e atualizações dos módulos, não será aceito o uso de ferramentas de terceiros;

**3.1.42** Permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.

**3.1.43** Possuir relatórios pré-configurados com filtros e conjuntos de filtros na console de gerenciamento.

**3.1.44** No console de gerenciamento em nuvem, a solução deve permitir a criação de relatórios customizados. Não serão aceitos apenas os relatórios pré-configurados da solução.

**3.1.45** Geração de relatórios, permitindo a customização dos mesmos e a exportação para os seguintes formatos (no mínimo um deles):

- **a)** CSV;
- **b)** PDF;

**3.1.46** Geração de relatórios que contenham as seguintes informações:

- **a)** Máquinas com a lista de definições de vírus desatualizada, ou todas as máquinas e suas respectivas versões da lista de definições de vírus;
- **b)** Versão do software instalado em cada máquina;
- **c)** Vírus que mais foram detectados;
- **d)** Máquinas que mais sofreram infecções em um determinado período de tempo;

**3.1.47** Permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes:

- **a)** Registro de eventos (log);
- **b)** Relatórios de eventos de vírus e status dos clientes;
- **c)** Relatórios de Softwares instalados;
- **d)** Relatórios de Hardware encontrados;

**3.1.48** Deve ter a capacidade de enviar eventos para um servidor SIEM, suportando no mínimo dois dos seguintes formatos:

**a)** JSON;

**b)** LEEF;

**c)** CEF;

**3.1.49** Fornecer, em tempo real, o status atualizado das estações de trabalho;

**3.1.50** Possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.

**3.1.51** Permitir a instalação remota do agente e produto de segurança através de GPO ou SCCM.

**3.1.52** Possuir módulo de gerenciamento de dispositivos móveis Android e iOS.

**3.1.53** Por meio do console de gerenciamento deve ser possível gerenciar dispositivos móveis iOS e Android e ter um banco de dados separado do restante dos servidores e estações de trabalho.

**3.1.54** O módulo de gerenciamento de dispositivos móveis deverá possuir arquitetura padrão de soluções MDM (Mobile Device Management) do mercado.

**3.1.55** A solução deverá disponibilizar o gerenciamento de dispositivos móveis também através do console em nuvem.

**3.1.56** O gerenciamento em dispositivos IOS deverá requerer certificado do serviço de notificação por push da Apple, a fim de possibilitar uma comunicação segura entre o servidor e o device.

**3.1.57** Possibilitar a instalação da solução de segurança aos dispositivos móveis de maneira manual através de QRcode, link gerado pela solução de gerenciamento e e-mail

**3.1.58** Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit por meio do módulo de firewall nas estações e servidores.

**3.1.59** Atualização incremental e on-line das vacinas.

**3.1.60** Atualização em clientes móveis (notebook, laptop, netbook, ultrabook e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador.

**3.1.61** Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet.

**3.1.62** Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante.

**3.1.63** Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.

**3.1.64** Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução.

**3.1.65** Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.

**3.1.66** O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.

**3.2 Solução de Antivírus para estações e servidores**

**3.2.1** A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.

**3.2.2** Gerenciado através de Console de Gerenciamento.

**3.2.3** Interface do software cliente em português.

**3.2.4** Manuais em português.

**3.2.5** O **cliente** para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação nos seguintes sistemas operacionais de **64 bits ou 32 bits, quando existentes, e versões posteriores, inclusive nas que forem lançadas durante a vigência do contrato**:

**a)** Microsoft Windows 7;

**b)** Microsoft Windows Server 2012 e R2;

**c)** Microsoft Windows Server 2016 (Server Core e Desktop Experience);

**d)** Ubuntu Desktop e Server 18.04 LTS

**e)** Red Hat Enterprise Linux 7;

**f)** Linux Mint 20;

**g)** CentOS 7;

**h)** Debian 10;

**i)** Alma Linux 8;

**j)** Rocky Linux 8;

**k)** SUSE Linux Enterprise Server (SLES) 15;

**l)** Oracle Linux 8;

**m)** Amazon Linux 2;

**n)** MacOS 10.15 Catalina Desktop e Server;

**o)** Android 6;

**p)** iOS 9;

**q)** iPadOS 13.

**3.2.6** O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.

**3.2.7** O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.

**3.2.8** Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante.

**3.2.9** Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.

**3.2.10** Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária.

**3.2.11** O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

**3.2.12** Atualização de configurações, sem interação (em background), nos clientes sem a necessidade de reinicialização ou logoff.

**3.2.13** Capacidade de tratar ameaças que exploram a ausência de correções do Sistema Operacional (patches) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja

instalada/disponível corretamente, ou possuir análise heurística ou inteligência artificial (machine learning) capaz de identificar e bloquear qualquer ameaça externa que se utilize de vulnerabilidades dos sistemas operacionais.

**3.2.14** Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça dia-zero, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.

**3.2.15** A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções:

**a)** Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples).

**b)** Pastas e arquivos pré-determinados através do caminho ou Hash.

**3.2.16** Deve permitir a instalação e desinstalação remota pela console de gerenciamento centralizada.

**3.2.17** Possibilidade de instalação presencial através de mídia de instalação fornecida ou gerada através do servidor de antivírus.

**3.2.18** Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo diária) e horários definidos no console de gerenciamento centralizado:

**a)** Permitir atualização incremental da lista de definições de vírus;

**b)** Permitir atualização por endereço do próprio fabricante, como opção além do servidor local;

**c)** Permitir configuração remota de ordem de preferência de endereços de atualização;

**d)** Permitir configurar conexão através de serviço Proxy local;

**e)** Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus.

**3.2.19** No sistema operacional Linux além de proteger e rastrear seus sistemas de arquivos, também aos arquivos armazenados em compartilhamentos SAMBA/CIFS ou que de alguma forma estejam disponibilizados para o acesso de clientes Windows em um servidor Linux.

**3.2.20** Deve ser capaz de detectar e remover todos os tipos de malwares, incluindo vírus, ransomware, worm, trojan, spyware, rootkit, vírus de macro e códigos maliciosos.

**3.2.21** Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como:

**a)** Machine Learning;

**b)** Instrusion Prevention System; e

**c)** Inteligência Artificial.

**3.2.22** Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.

**3.2.23** Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.

**3.2.24** Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.

**3.2.25** A solução para estações de trabalho Windows deve possuir módulo com funcionalidade de navegador seguro, para proteção de acesso a websites que contenham dados confidenciais. Não serão aceitos módulos convencionais de “Web Protection”, deverá oferecer camada adicional dedicada para tal proteção.

**3.2.26** Empregar proteção baseada em nuvem conectada diretamente aos laboratórios de pesquisa e desenvolvimento do fabricante.

**3.2.27** Possuir módulo nativo de detecção e proteção contra variantes de ransomware existentes no mundo, a fim de atuar como um escudo contra este tipo de ameaça.

**3.2.28** A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso.

**3.2.29** Permitir diferentes configurações de varredura em tempo real, tornando o desempenho do produto mais estável, principalmente em máquinas com baixo desempenho de hardware.

**3.2.30** Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.

**3.2.31** Detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração

remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.

**3.2.32** Rastreamento manual com interface gráfica, customizável, com opção de limpeza.

**3.2.33** Rastreamento por linha de comando, parametrizável, com opção de limpeza.

**3.2.34** Programação de rastreamentos automáticos do sistema com as seguintes opções:

**a)** Escopo: todos os drives locais, específicos ou pastas específicas;

**b)** Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança;

**c)** Frequência: diária, semanal e mensal;

**d)** Exclusões: pastas ou arquivos que não devem ser rastreados;

**3.2.35** Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando.

**3.2.36** Detecção de anomalias através dos métodos de assinatura, heurística e por comportamento.

**3.2.37** Proteção contra ameaças via internet. A solução deve conter pelo menos:

**a)** Ajuste no nível de sensibilidade da detecção;

**b)** Lista de exceção.

**3.2.38** Detecção em tempo real e possibilidade de bloqueio e remoção de malwares provenientes de downloads realizados no ambiente web.

**3.2.39** Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser desabilitada;

**3.2.40** Detecção em tempo real e possibilidade de bloqueio e remoção de malwares no conteúdo e anexos de mensagens de correio eletrônico, pelo antivírus cliente, analisando tráfego e suportando principais clientes (no mínimo outlook).

**3.2.41** Permitir que a funcionalidade de rastreamento em tempo real de e-mail possa ser desabilitada.

**3.2.42** Detecção em tempo real e possibilidade de bloqueio e remoção de malwares nas áreas de armazenamento de dispositivos removíveis, tais como:

**a)** PenDrive;

**b)** HD externo;

**c)** Celulares;

**d)** Tablets;

**e)** CD/DVD;

**f)** Impressora USB;

**g)** Armazenamento de FireWire;

**h)** Dispositivo Bluetooth;

**i)** Leitor de cartão inteligente;

**j)** Dispositivo de criação de imagem;

**k)** Modem;

**l)** Porta LPT/COM;

**m)** Dispositivo portátil;

**3.2.43** O módulo de controle de dispositivos deve estar disponível para estações de trabalho Windows, macOS e Linux.

**3.2.44** Detecção, varredura, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação, nos formatos mais utilizados no mercado.

**3.2.45** Ferramenta de firewall bidirecional local no cliente, com possibilidade de configuração, ativação e desativação através da console de gerenciamento centralizada, contendo filtros especificados por aplicação, protocolo, IP, range de IPs, rede, porta e range de portas.

**3.2.46** A ferramenta de firewall local deverá tratar tráfego de entrada e de saída de forma independente.

**3.2.47** Deve permitir o bloqueio do “Autorun” nas portas USB ou bloquear automaticamente a execução de qualquer ameaça em dispositivos móveis.

**3.2.48** Permitir bloquear a conexão de dispositivos removíveis.

**3.2.49** Gerar registro (log) dos eventos de vírus em arquivo.

**3.2.50** Gerar relatórios, ao menos, de:

**a)** Eventos de vírus;

**b)** Status dos clientes;

**c)** Status dos Updates;

**3.2.51** Gerar notificações de eventos de vírus através de alerta por e-mail, ao menos.

**3.2.52** Gerar relatórios incluindo tipos de vírus, nome do vírus e se precisa de atualização do Sistema Operacional.

**3.2.53** 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.

**3.2.54** Permitir a criação de exceções nos escaneamentos de arquivos.

**3.2.55** Permitir o bloqueio de dispositivos com base nos seguintes critérios:

**a)** Fabricante;

**b)** Modelo;

**c)** Número de série;

**3.2.56** Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.

**3.2.57** A solução deve permitir a configuração de quais portas HTTPs serão escaneadas para verificação de conexões criptografadas.

**3.2.58** O Firewall deve possuir funcionalidade de suportar os protocolos TCP e UDP.

**3.2.59** O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.

**3.2.60** Possuir proteção contra-ataques de Denial of Service (DoS), Port-Scan e Spoofing e botnet.

**3.2.61** Possibilidades de criação de assinaturas personalizadas para detecção.

**3.2.62** Possibilidade de agendar a ativação de novas regras do firewall.

**3.2.63** Possibilidade de criar regras diferenciadas por aplicações.

**3.2.64** Bloqueio de ataques baseado na exploração da vulnerabilidade.

**3.2.65** Permitir integração com navegadores WEB para prevenção de ataques.

**3.2.66** Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.

**3.2.67** Possuir taxa de performance de rede inferior a 70MB (megabytes) comprovada junto a instituições reconhecidas mundialmente em análises profundas de funcionalidades de fabricantes de soluções de segurança.

**3.2.68** A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.

**3.2.69** As configurações do antimalware deverão ser realizadas através do mesma console de todos os itens da solução.

**3.2.70** Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).

**3.2.71** Permitir verificação das ameaças de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do sistema operacional fornecendo a possibilidade de detecção de Rootkits.

**3.2.72** Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos, com intervalos de tempo determinados, de forma a reduzir impacto em ambientes.

**3.2.73** Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.

**3.2.74** Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP.

**3.2.75** Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos, mesmo que sejam compactados.

**3.2.76** Capacidade de terminar o processo e serviço da ameaça no momento de detecção.

**3.2.77** Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.

**3.2.78** Possibilidade de bloquear verificação de malware em recursos mapeados da rede.

**3.2.79** Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.

**3.2.80** Não serão aceitas soluções de Antimalware que possuam engine de terceiros.

**3.2.81** Permitir o bloqueio da execução de aplicações baseado em nome e pasta.

**3.2.82** A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações.

**3.2.83** Capacidade de detecção de keyloggers por comportamento dos processos em memória.

**3.2.84** Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts.

**3.2.85** Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.

**3.2.86** Realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como:

**a)** Aprendizado de máquina;

**b)** Deep Learning;

**c)** Análise estatística e dinâmica;

**d)** Detecção baseada em comportamento;

**e)** Introspecção na memória;

**3.2.87** Detecção do malware por DNA do vírus.

**3.2.88** Deverá ter a capacidade de atualizar os patches do sistema operacional.

**3.2.89** A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hypervisor.

**3.2.90** Em servidores que usam “OneDrive for Business” deve ser possível explorar os arquivos armazenados nesta nuvem, procurando por arquivos comprometidos ou possível malware.

**3.2.91** A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços que foram identificados com este comportamento malicioso.

**3.2.92** A solução deve adicionar exclusões automaticamente para aplicativos de servidor críticos.

**3.2.93** A solução deve possuir otimização de desempenho para infraestruturas mistas (física e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.

**3.2.94** Controlar acesso a sites, possibilitando o bloqueio dos mesmos.

**3.2.95** Permitir criar políticas de bloqueio com base em categorias e lista de URL.

**3.2.96** Permitir gerar relatórios de sites acessados e bloqueados.

**3.2.97** Permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.

**3.2.98** Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.

**3.2.99** Para o módulo de proteção de e-mail, deve suportar minimamente os seguintes protocolos:

**a)** POP3;

**b)** POP3S;

**c)** IMAP;

**d)** IMAPS;

**3.2.100** Deve permitir a configuração de ações personalizadas para detecções realizadas pelo módulo de proteção de e-mail, suportando minimamente as seguintes ações:

**a)** Mover o e-mail para uma pasta;

**b)** Excluir o e-mail;

**c)** Manter o e-mail;

**3.2.101** Em equipamentos macOS, a solução deve possuir módulo para proteção de e-mails de entrada e saída.

**3.2.102** Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.

**3.2.103** A solução de proteção antispam deve realizar as verificações utilizando o protocolo SSL.

**3.2.104** O módulo de proteção antispam deverá ser nativo e integrado ao Endpoint.

**3.2.105** Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push.

**3.3 Solução de Sandbox em nuvem**

**3.3.1** Deve ser possível criar exclusões por caminho, nome de detecção e hash do arquivo (SHA-1).

**3.3.2** A solução deve permitir a definição do tempo máximo para análise automática de artefatos.

**3.3.3** Capacidade de sincronizar seu licenciamento com a nuvem e o console de administração no local (on-premise) ou na nuvem.

**3.3.4** Detectar um arquivo suspeito executado pela primeira vez, um aviso deve ser exibido, se a verificação for concluída antes do arquivo ser executado pela primeira vez, o aviso de arquivo sob verificação não será exibido. Deve eliminar automaticamente as amostras dos arquivos/executáveis nos servidores onde o comportamento foi analisado.

**3.3.5** Capacidade para enviar e-mails de SPAM para sua análise.

**3.3.6** Deve classificar os artefatos em categorias, oferecendo no mínimo as seguintes categorias: desconhecido, limpo, suspeito, altamente suspeito e malicioso.

**3.3.7** Deve disponibilizar as seguintes informações de um arquivo enviado ao Sandbox na nuvem: nome do equipamento que enviou o arquivo, o usuário conectado no dispositivo, o resultado da análise, hash no formato SHA-1, nome do arquivo analisado, tamanho do arquivo, categoria.

**3.3.8** Deve oferecer proteção proativa, ou seja, que o arquivo/executável seja bloqueado até receber o resultado do Sandbox na nuvem.

**3.3.9** A solução deve possuir integração com a solução de antimalware, para possuir maiores possibilidades de proteção e aplicação de políticas.

**3.3.10** A solução de Sandbox em nuvem deve estar disponível minimamente para integração com os produtos para estações e servidores Windows e Linux.

**3.3.11** Deve ser possível enviar um arquivo/executável manualmente para a solução de Sandbox em nuvem.

**3.4 Solução para criptografia de discos**

**3.4.1** A solução deverá ser capaz de criptografar dispositivos Windows e macOS.

**3.4.2** Para estações Windows, a solução deverá possuir tecnologia própria de criptografia. Não serão aceitas soluções que apenas oferecem gerenciamento do BitLocker (Microsoft).

**3.4.3** Para estações macOS, a solução deve ser capaz de gerenciar o FileVault, disponibilizado pela Apple.

**3.4.4** A solução deverá ser capaz de criptografar os Endpoints desejados desde o início do sistema operacional.

**3.4.5** A solução deverá dispor de diversas possibilidades de recuperação de senha para usuários remotos que estejam bloqueados.

**3.4.6** A solução deverá poder programar as tarefas de criptografia sobre os Endpoints desejados com a possibilidade de pausar a execução para retomar desde o último estado.

**3.4.7** A solução deverá ser administrada desde o mesmo console central junto com as outras soluções descritas neste termo de referência.

**3.4.8** Possibilitar a opção de criptografar apenas o disco de inicialização.

**3.4.9** Possibilitar que as estações de trabalho sejam criptografas sem que o recurso de TPM (Trusted Platform Module) esteja válido.

**3.4.10** Através da console central deve ser possível invalidar a senha de login do usuário e solicitar que mude sua senha de login por meio de uma interface gráfica.

**3.4.11** Deve possibilitar que o administrador recupere os dados caso o usuário não consiga acessar a máquina com suas credenciais.

**3.4.12** Deve possibilitar que o administrador gere uma nova senha de recuperação para o usuário.

**3.5 Outros requerimentos gerais**.

**3.5.1** A solução ofertada não deve possuir restrições sobre a quantidade de equipamentos para ativação das licenças. A totalidade das licenças contratadas pode ser ativada completamente em servidores, estações de trabalho, ou dispositivos móveis, respeitando o limite total contratado.

**3.5.2** Todos os módulos ofertados pelo fabricante, devem ser ativados utilizando uma única licença, sem a necessidade de aquisição de módulos separados (add-ons).

**3.5.3** O fabricante deve comprovar premiações e participações em programas de certificação.

**3.5.4** O fabricante deverá ter suporte local em idioma português.

**3.5.5** O fabricante deve oferecer serviços de segurança da informação como por exemplo: teste de penetração, avaliação de vulnerabilidade ou análise de GAPs.

**3.5.6** O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.

**3.5.7** O fabricante deve possuir escritório próprio no Brasil.

**3.5.8** Possuir manuais de apoio sobre a solução em português.

**3.5.9** O fabricante deverá ter documentação publicada na internet no idioma português.

**3.5.10** O fabricante deve contar com a certificação de segurança ISO 27001.

**Da Compatibilidade com Sistemas Legados:**

**a)** A operacionalidade da Solução em Sistemas Legados (por exemplo: Windows 7, 8.1) será garantida pelo uso de *engines* de versões anteriores buscando, se possível, o gerenciamento único.

## 4 Estimativas das quantidades a serem adquiridas/contratadas

| ITEM | DESCRIÇÃO | UNIDADE | CONSUMO 2023 | ESTIMADO 2024 |
|---|---|---|---|---|
| **1** | SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, CONFORME ESPECIFICAÇÕES ANEXAS. | **LICENÇA** | **1900** | **2.000** |

Foi estimada a contratação de 2000 licenças de uso para instalação nos equipamentos físicos e máquinas virtuais da UNITAU, devido a aquisição de novos equipamentos.

## 5 Levantamento das soluções existentes no mercado

Foram avaliadas soluções de segurança corporativa para endpoints que garantam a segurança dos dados e informações de propriedade ou sob custódia das áreas de negócio da UNITAU.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

## 6 Análise das alternativas e escolha da solução mais adequada

A contratação deverá ser feita considerando a melhor opção de segurança.

## 7 Resultados pretendidos

Garantir o acesso, a segurança e a propriedade dos dados, sistemas e equipamentos de propriedade ou sob custódia das áreas de negócio da Universidade de Taubaté.

## 8 Estimativa do valor da aquisição/contratação

O Total estimado da aquisição é de R$ 431.720,00 (quatrocentos e trinta e um mil, setecentos e vinte reais) para o período de cinco anos.

Para estimar o valor supracitado, foi realizada consulta a empresas fornecedoras de soluções de segurança para TI.

**Órgão:** CONSELHO FEDERAL DE CONTABILIDADE

**Id contratação PNCP:** 33618570000107-1-000016/2024

Valor anual -R$ 84.670,80

**Órgão:** CONSELHO FEDERAL DE CONTABILIDADE

**Id contratação PNCP:** 33618570000107-1-000024/2023

Valor anual -R$ 87.412,50

“O valor apresentado neste estudo foi atualizado em razão do tempo decorrido desde a elaboração do PAC.”

**A estimativa atualizada constará em anexo**, após pesquisa de preços a ser realizada pelo Serviço de Licitações e Compras, conforme parâmetros estabelecidos nos incisos I, II, III, IV e V, do §1º, artigo 23, da Lei Federal nº 14.133/2021 e validação deste Setor.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

## 9 Descrição da solução como um todo

Para atendimento à demanda, deverá ser contratada solução de segurança corporativa para endpoints, conforme especificações do termo de referência,que inclua suporte presencial/remoto para instalação, configuração, customização e eventuais treinamentos que se fizerem necessários, conforme especificações técnicas e demais requisitos indicados nos itens 3 e 4 deste ETP.

**A validade da contratação será de 60 meses.**

## 10 Justificativas para o parcelamento ou não da contratação

Considerando a natureza do objeto, e por se tratar de **ITEM**, não cabe o parcelamento.

## 11 Providências prévias a serem adotadas pela Administração

Não há providências prévias para a contratação pretendida.

## 12 Contratações correlatas e/ou interdependentes

Não há aquisições/contratações correlatas ou interdependentes para a contratação pretendida.

## 13 Descrição de possíveis impactos ambientais e respectivas medidas mitigadoras

Não se aplica.

## 14 Políticas de realocação de equipamentos e descarte

Não se aplica.

## 15 Áreas requisitantes

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

Central de Tecnologia da Informação.

**16 Responsável pela elaboração:**

Servidor: Reginaldo Adriane da Silva Gazzi

Cargo: Analista de Sistema Sênior

Telefone: 3625.4114

e-mail: infra@unitau.br

Taubaté, 12/08/2024

Reginaldo Adriane da Silva Gazzi
Analista de Sistema Sênior

**17 Responsável pelo Departamento/Setor:**

Declaro a viabilidade técnica da contratação apresentada neste Estudo **técnico Preliminar, para atendimento da demanda apresentada**.

Encaminhe-se à **Pró-reitoria de Administração** para **avaliação e parecer.**

**Jaqueline Blanco**
**Coordenadora da Central de T. I.**

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**18 Posicionamento conclusivo dos setores responsáveis pelo Planejamento da Instituição, sobre a adequação da contratação para o atendimento da necessidade a que se destina (*)**

O presente estudo técnico preliminar evidencia que a contratação da solução descrita no item 6 "**Análise das alternativas e escolha da solução mais adequada"** se **mostra tecnicamente viável, fundamentadamente necessária e alinhada com o Planejamento desta unidade**.

Diante do exposto, **DECLARO QUE É VIÁVEL** *a presente contratação.*

**A aquisição pretendida está alinhada com os objetivos dispostos no Plano Plurianual 2022-2025, e com as metas estabelecidas na Lei Orçamentária Anual do exercício de 2024, quais sejam:**

Realização do suporte administrativo necessário à manutenção e ao desenvolvimento dos objetivos da Instituição, garantindo estrutura adequada para apoio às ações de conservação, limpeza, vigilância dos espaços físicos, serviços de recursos humanos, planejamento, compras, patrimônio, almoxarifado, transportes, telefonia, protocolo e expediente geral, informática, serviços gráficos, comunicações, manutenção de equipamentos eletroeletrônicos, ópticos, de climatização e de refrigeração, entre outras.

Taubaté, 12/08/2024

**Prof. Dr. Renato Rocha**
**Pró-reitor de Administração**

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# ANEXO IV

# MAPA DE RISCOS

**UNIVERSIDADE DE TAUBATÉ**

**MAPA DE RISCOS**

**UNIDADE ORÇAMENTÁRIA:** PRÓ-REITORIA DE ADMINISTRAÇÃO
**DEPARTAMENTO:** Central de Tecnologia da Informação
**OBJETO:** Aquisição de solução de segurança corporativa para endpoints, servidores e rede UNITAU conforme especificações deste termo de referência, contemplando suporte presencial/remoto para instalação, configuração, customização e treinamento, por 60 meses
**Documento:** ETP CETI Nº 10/2024

| RISCO | Descrição do Risco | EFEITO | FASE | Categoria | Probabilidade de Ocorrência | Impacto | Severidade | Ação | AÇÃO PREVENTIVA | Responsável | AÇÃO DE CONTINGÊNCIA | Responsável |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Impugnações do Edital de licitação | 1.Possibilidade de impugnações do edital na fase de seleção do fornecedor<br>2. Atraso na contratação | SELEÇÃO DO FONECEDOR | Operacionais | 1-BAIXO | 2-MÉDIO | BAIXO | Mitigar | 1. revisão dos artefatos para identificar e ajustar os pontos que possam incorrer em questionamentos | Requisitante/Equipe de planejamento da Contratação | 1.Em casos de impugnações por condições indevidas solicitar aos responsáveis que procedam com as correções.<br>2.Republicação do Edital, com a reabertura da contagem de prazos. | 1.Requisitante/Equipe de Planejamento da Contratação<br>2. Serviço de Licitações e Compras |
| 2 | LICITAÇÃO DESERTA - caso nenhuma empresa se interesse por sua execução | 1. Necessidade de republicação da licitação, impactando no planejamento do Setor de Licitações<br>2.Atraso na contratação | SELEÇÃO DO FONECEDOR | Operacionais | 1-BAIXO | 2-MÉDIO | BAIXO | Mitigar | Correto planejamento das exigências e condições estabelecidas para a contratação | Requisitante/Equipe de planejamento da Contratação | Verificar junto às empresas do ramo de atividade quais seriam os motivos do desinteresse pelo serviço para uma possível repetição do certame | Requisitante/Serviço de Licitações e Compras |
| 3 | LICITAÇÃO FRACASSADA - caso nenhuma das propostas apresentadas esteja dentro dos parâmetros estimados pela Administração | 1. Necessidade de republicação da licitação, impactando no planejamento do Setor de Compras<br>2.Atraso na contratação | SELEÇÃO DO FONECEDOR | Operacionais | 1-BAIXO | 2-MÉDIO | BAIXO | Mitigar | Correto planejamento das exigências e condições estabelecidas para a contratação | Requisitante/Equipe de planejamento da Contratação | Verificar junto às empresas do ramo de atividade quais seriam os motivos do desinteresse pelo serviço e revisão dos valores estimados para uma possível repetição do certame | Serviço de Licitações e Compras |
| 4 | A empresa vencedora do certame quando convocada, não assinar o contrato administrativo | Atraso na contratação e possível não atendimento da demanda na data prevista | EXECUÇÃO CONTRATUAL | Operacionais | 1-BAIXO | 3-ALTO | MEDIO | Mitigar | 1. Prever, dentre as cláusulas do Edital, sanções que contemplem esta situação. | Requisitante/Equipe de planejamento da Contratação | 1. Convocar o segundo colocado para possível contratação<br>2. Aplicar as sanções cabíveis | 1. Serviço de Licitações e Compras<br>2.Setor de Contratos |

# UNIVERSIDADE DE TAUBATÉ

## MAPA DE RISCOS

**UNIDADE ORÇAMENTÁRIA:** PRÓ-REITORIA DE ADMINISTRAÇÃO
**DEPARTAMENTO:** Central de Tecnologia da Informação
**OBJETO:** Aquisição de solução de segurança corporativa para endpoints, servidores e rede UNITAU conforme especificações deste termo de referência, comtemplando suporte presencial/remoto para instalação, configuração, customização e treinamento, por 60 meses
**Documento:** ETP CETI Nº 10/2024

| RISCO | Descrição do Risco | EFEITO | FASE | Categoria | Probabilidade de Ocorrência | Impacto | Severidade | Ação | AÇÃO PREVENTIVA | Responsável | AÇÃO DE CONTINGÊNCIA | Responsável |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | Não cumprimento dos prazos de entrega | não atendimento da demanda, podendo causar prejuízos a instituição | EXECUÇÃO CONTRATUAL | Operacionais e financeiros | 1-BAIXO | 3-ALTO | MÉDIO | Mitigar | 1. Prever, dentre as cláusulas do Edital, sanções que contemplem esta situação. | Requisitante/Equipe de planejamento da Contratação | Instaurar processo para aplicação de penalidades à Contratada. | Fiscal Técnico do Setor requisitante e Setor de Contratos |

**Reginaldo Adriane da Silva Gazzi**
Analista de Sistema Sênior

**Jaqueline Blanco**
Coordenadora de Central de T.I.

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# ANEXO V

# TERMO DE REFERÊNCIA

## Central de Tecnologia da Informação

## Aquisição de serviços

## Aquisição de serviços

### (01) Objeto

Aquisição de Solução de segurança corporativa para endpoints, servidores e rede UNITAU conforme especificações deste termo de referência, contemplando suporte presencial/remoto para instalação, configuração, customização e treinamento, por 60 meses.

### (02) Motivação

Na tecnologia de informação e comunicação (TIC) as ameaças à segurança têm crescido de forma galopante nos últimos anos. Hoje são necessárias várias camadas de proteção tanto na rede, servidores, e-mails, computadores e até smartphones. A solução que pretendemos adquirir deve completar de forma mais justa e eficiente as outras camadas que já dispomos de segurança e as que planejamos adquirir. Nos ataques mundiais de ransomware ocorridos ultimamente ficou clara a necessidade de backup, proteção dos endpoints e atualização dos sistemas operacionais (de uma forma bastante resumida). Outras soluções poderão superpor medidas já utilizadas ou deixar outras sem nenhuma cobertura. Portanto, uma solução de segurança complementar às já existentes. Não devendo duplicar funções já existentes, mas cobrir as áreas ainda não contempladas pelas outras camadas de soluções. É fundamental manter recursos tecnológicos que garantam a segurança dos dados e informações de propriedade ou sob custódia das áreas de negócio da UNITAU, haja vista a necessidade fundamental de proteção dos dados, de grande valor para a instituição, contra os mais diversos tipos de ameaças.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**(03) Especificações técnicas**

As empresas licitantes deverão informar claramente na Proposta a marca e modelo da solução, sob pena de desclassificação.

| Item | Descrição | Qtd |
|---|---|---|
| 01 | SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, CONFORME ESPECIFICAÇÕES ANEXAS | 2000 |

Solução de segurança corporativa para endpoints, conforme especificações do termo de referência, inclui suporte presencial/remoto para instalação, configuração, customização e eventuais treinamentos que se fizerem necessários ao longo dos 60 meses.

Aquisição de software de proteção antivírus, com funcionalidades antispyware, de controle de dispositivos, de prevenção de intrusos (IPS) e firewall para rede, estações de trabalho e servidores de arquivos/aplicações da UNITAU, sendo máquinas físicas ou virtuais e em ambiente local ou em nuvem, incluindo: instalação e configuração dos softwares da solução, incluindo desinstalações de softwares anteriores, se for o caso; Operação assistida de funcionamento da solução; atualização de software e base de assinaturas; treinamento presencial ou on-line, em português, com interação entre as partes, para 6 (seis) servidores da UNITAU e treinamentos contínuos online em plataforma web própria tanto da solução adquirida, quanto das demais soluções para ampliação de conhecimentos técnicos; os treinamentos serão aceitos de forma on-line desde que a Contratada, ofereça ferramentas e ambientes para simulação e configuração conforme a estrutura verificada no momento da instalação na UNITAU. Além disso, os treinamentos e/ou reuniões on-line deverão ser gravados e disponibilizados para consultas posteriores; e suporte técnico pelo período de 60 (sessenta) meses, conforme especificações deste Termo de Referência.

**3.6 Console de gerenciamento centralizado**

**3.6.1** O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor.

**3.6.2** O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS) compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.

**3.6.3** O acesso ao Console deve suportar várias sessões simultâneas.

**3.6.4** Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.

**3.6.5** Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor.

**3.6.6** Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.

**3.6.7** O **servidor de gerenciamento** deve possuir compatibilidade para instalação nos seguintes sistemas operacionais, **de 64 bits ou 32 bits, quando existentes, e versões posteriores, inclusive nas que foram lançadas durante a vigência do contrato,** bem como em todas as versões/distribuições/releases e Hypervisors:

**n)** Microsoft Windows 7;

**o)** Microsoft Windows Server 2012 e R2;

**p)** Microsoft Windows Server 2016 (Server Core e Desktop Experience);

**q)** Ubuntu 18.04.1 LTS Desktop e Server;

**r)** Red Hat Enterprise Linux 7;

**s)** CentOS 7;

**t)** Debian 10;

**u)** VMware vSphere/ESXi 6.5;

**v)** VMware Workstation 9;

**w)** VMware Player 7;

**x)** Microsoft Hyper-V Server 2012;

**y)** Oracle VirtualBox 6.0;

**z)** Citrix 7.0 e posterior.

**3.6.8** O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE, ou seja, será instalado completamente no ambiente da UNITAU e também ter a opção de gerenciamento em nuvem, pois temos máquinas em redes internas sem acesso a Internet e também com acesso a Internet e sem acesso a rede interna.

**3.6.9** O console de gerenciamento deve oferecer também, opção para gerenciamento em nuvem, disponibilizado pela CONTRATADA.

**3.6.10** Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.

**3.6.11** Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.

**3.6.12** Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.

**3.6.13** Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso).

**3.6.14** Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.

**3.6.15** Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.

**3.6.16** Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

**3.6.17** O console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.

**3.6.18** Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador).

**3.6.19** A solução deve possuir sistema RBAC (Role Based Access Control) para definir acessos customizados de usuários adicionais no console, oferecendo granularidade para configuração dos acessos, para segregar os acessos, limitando os acessos a não exclusivamente políticas, tarefas, e demais objetos do console.

**3.6.20** O log deve ser centralizado e conter, no mínimo, os seguintes itens:

**j)** Nome da ameaça;

**k)** Nome do arquivo infectado;

**l)** Caminho da detecção;

**m)** HASH do arquivo;

**n)** Data e hora da infecção;

**o)** Ação tomada;

**p)** Endereço de IP da máquina;

**q)** Usuário autenticado na máquina;

**r)** Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado;

**3.6.21** Fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações:

**g)** Nome da máquina;

**h)** Endereço IP da máquina;

**i)** Malwares não removidos;

**j)** Status da conexão;

**k)** Data da vacina;

**l)** Versão do antivírus instalado.

**3.6.22** O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques. Suportando no mínimo alertas dos seguintes módulos:

**d)** Detecções de Malware;

**e)** Detecções de Firewall;

**f)** Detecções via EDR;

**3.6.23** Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.

**3.6.24** Capacidade de voltar (rollback) para versão de atualização (da solução ou vacina) através de procedimento específico no console de gerenciamento.

**3.6.25** Interface da Console de Gerenciamento totalmente em português.

**3.6.26** Deve permitir criar o backup da Base de dados da Console de gerenciamento.

**3.6.27** O acesso ao console de gerenciamento deverá ser autenticado.

**3.6.28** A console deverá funcionar também através de um Appliance Virtual fornecido pelo fabricante.

**3.6.29** O acesso ao console de administração do antivírus deve permitir a possibilidade de ser feito com duplo fator de autenticação integrado dentro da

mesma console onde é possível ativá-lo sem a necessidade de nenhum add-on adicional.

**3.6.30** Gerar pacotes de instalação dos clientes, para cada tipo de sistema operacional existente na estrutura da CONTRATANTE, possibilitando a gravação em mídia e a instalação do software em ambientes onde não seja possível a instalação via rede corporativa.

**3.6.31** Permitir forçar a instalação do software cliente do antivírus nos computadores, reinstalando-o em caso de desinstalação ou corrupção do mesmo.

**3.6.32** Atualização de vacinas sem a necessidade de reinicialização.

**3.6.33** Suportar o gerenciamento de todos os clientes instalados nas máquinas (estações de trabalho, servidores, tablets e smartphones) a partir do servidor de Console de Gerenciamento, oferecendo a possibilidade de configuração centralizada e remota de todas as funcionalidades.

**3.6.34** Gerenciar de forma remota as configurações do firewall local de cada máquina com o cliente instalado.

**3.6.35** A solução deve oferecer recurso para isolar as máquinas da rede, mantendo apenas comunicação segura com o servidor de gerenciamento.

**3.6.36** Criação de grupos e subgrupos de máquinas baseada na hierarquia do Active Directory e LDAP ou em identificador único de clientes, tal como endereço IP;

**3.6.37** Forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada na console de gerenciamento.

**3.6.38** Atualização/sincronização de configurações nos clientes sem a necessidade de reinicialização ou logoff.

**3.6.39** Permitir a criação de tarefas de rastreamento em períodos de tempo pré-determinados e na inicialização do sistema operacional.

**3.6.40** Permitir a criação de tarefas de atualização de vacinas e novas versões de software em períodos de tempo pré-determinados.

**3.6.41** Permitir o uso de ferramentas para centralizar a distribuição de atualizações de software e atualizações dos módulos, não será aceito o uso de ferramentas de terceiros;

**3.6.42** Permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.

**3.6.43** Possuir relatórios pré-configurados com filtros e conjuntos de filtros na console de gerenciamento.

**3.6.44** No console de gerenciamento em nuvem, a solução deve permitir a criação de relatórios customizados. Não serão aceitos apenas os relatórios pré-configurados da solução.

**3.6.45** Geração de relatórios, permitindo a customização dos mesmos e a exportação para os seguintes formatos (no mínimo um deles):

**c)** CSV;

**d)** PDF;

**3.6.46** Geração de relatórios que contenham as seguintes informações:

**e)** Máquinas com a lista de definições de vírus desatualizada, ou todas as máquinas e suas respectivas versões da lista de definições de vírus;

**f)** Versão do software instalado em cada máquina;

**g)** Vírus que mais foram detectados;

**h)** Máquinas que mais sofreram infecções em um determinado período de tempo;

**3.6.47** Permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes:

**e)** Registro de eventos (log);

**f)** Relatórios de eventos de vírus e status dos clientes;

**g)** Relatórios de Softwares instalados;

**h)** Relatórios de Hardware encontrados;

**3.6.48** Deve ter a capacidade de enviar eventos para um servidor SIEM, suportando no mínimo dois dos seguintes formatos:

**a)** JSON;

**b)** LEEF;

**c)** CEF;

**3.6.49** Fornecer, em tempo real, o status atualizado das estações de trabalho;

**3.6.50** Possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.

**3.6.51** Permitir a instalação remota do agente e produto de segurança através de GPO ou SCCM.

**3.6.52** Possuir módulo de gerenciamento de dispositivos móveis Android e iOS.

**3.6.53** Por meio do console de gerenciamento deve ser possível gerenciar dispositivos móveis iOS e Android e ter um banco de dados separado do restante dos servidores e estações de trabalho.

**3.6.54** O módulo de gerenciamento de dispositivos móveis deverá possuir arquitetura padrão de soluções MDM (Mobile Device Management) do mercado.

**3.6.55** A solução deverá disponibilizar o gerenciamento de dispositivos móveis também através do console em nuvem.

**3.6.56** O gerenciamento em dispositivos IOS deverá requerer certificado do serviço de notificação por push da Apple, a fim de possibilitar uma comunicação segura entre o servidor e o device.

**3.6.57** Possibilitar a instalação da solução de segurança aos dispositivos móveis de maneira manual através de QRcode, link gerado pela solução de gerenciamento e e-mail

**3.6.58** Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit por meio do módulo de firewall nas estações e servidores.

**3.6.59** Atualização incremental e on-line das vacinas.

**3.6.60** Atualização em clientes móveis (notebook, laptop, netbook, ultrabook e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador.

**3.6.61** Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet.

**3.6.62** Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante.

**3.6.63** Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.

**3.6.64** Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução.

**3.6.65** Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.

**3.6.66** O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.

**3.7 Solução de Antivírus para estações e servidores**

**3.7.1** A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.

**3.7.2** Gerenciado através de Console de Gerenciamento.

**3.7.3** Interface do software cliente em português.

**3.7.4** Manuais em português.

**3.7.5** O **cliente** para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação nos seguintes sistemas operacionais de **64 bits ou 32 bits, quando existentes, e versões posteriores, inclusive nas que forem lançadas durante a vigência do contrato**:

**r)** Microsoft Windows 7;

**s)** Microsoft Windows Server 2012 e R2;

**t)** Microsoft Windows Server 2016 (Server Core e Desktop Experience);

**u)** Ubuntu Desktop e Server 18.04 LTS

**v)** Red Hat Enterprise Linux 7;

**w)** Linux Mint 20;

**x)** CentOS 7;

**y)** Debian 10;

**z)** Alma Linux 8;

**aa)** Rocky Linux 8;

**bb)** SUSE Linux Enterprise Server (SLES) 15;

**cc)** Oracle Linux 8;

**dd)** Amazon Linux 2;

**ee)** MacOS 10.15 Catalina Desktop e Server;

**ff)** Android 6;

**gg)** iOS 9;

**hh)** iPadOS 13.

**3.7.6** O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.

**3.7.7** O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.

**3.7.8** Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante.

**3.7.9** Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.

**3.7.10** Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária.

**3.7.11** O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

**3.7.12** Atualização de configurações, sem interação (em background), nos clientes sem a necessidade de reinicialização ou logoff.

**3.7.13** Capacidade de tratar ameaças que exploram a ausência de correções do Sistema Operacional (patches) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja instalada/disponível corretamente, ou possuir análise heurística ou inteligência artificial (machine learning) capaz de identificar e bloquear qualquer ameaça externa que se utilize de vulnerabilidades dos sistemas operacionais.

**3.7.14** Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça dia-zero, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.

**3.7.15** A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções:

**c)** Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples).

**d)** Pastas e arquivos pré-determinados através do caminho ou Hash.

**3.7.16** Deve permitir a instalação e desinstalação remota pela console de gerenciamento centralizada.

**3.7.17** Possibilidade de instalação presencial através de mídia de instalação fornecida ou gerada através do servidor de antivírus.

**3.7.18** Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo diária) e horários definidos no console de gerenciamento centralizado:

**a)** Permitir atualização incremental da lista de definições de vírus;

**b)** Permitir atualização por endereço do próprio fabricante, como opção além do servidor local;

**c)** Permitir configuração remota de ordem de preferência de endereços de atualização;

**d)** Permitir configurar conexão através de serviço Proxy local;

**e)** Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus.

**3.7.19** No sistema operacional Linux além de proteger e rastrear seus sistemas de arquivos, também aos arquivos armazenados em compartilhamentos SAMBA/CIFS ou que de alguma forma estejam disponibilizados para o acesso de clientes Windows em um servidor Linux.

**3.7.20** Deve ser capaz de detectar e remover todos os tipos de malwares, incluindo vírus, ransomware, worm, trojan, spyware, rootkit, vírus de macro e códigos maliciosos.

**3.7.21** Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como:

**a)** Machine Learning;

**b)** Instrusion Prevention System; e

**c)** Inteligência Artificial.

**3.7.22** Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.

**3.7.23** Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.

**3.7.24** Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.

**3.7.25** A solução para estações de trabalho Windows deve possuir módulo com funcionalidade de navegador seguro, para proteção de acesso a websites que contenham dados confidenciais. Não serão aceitos módulos convencionais de "Web Protection", deverá oferecer camada adicional dedicada para tal proteção.

**3.7.26** Empregar proteção baseada em nuvem conectada diretamente aos laboratórios de pesquisa e desenvolvimento do fabricante.

**3.7.27** Possuir módulo nativo de detecção e proteção contra variantes de ransomware existentes no mundo, a fim de atuar como um escudo contra este tipo de ameaça.

**3.7.28** A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso.

**3.7.29** Permitir diferentes configurações de varredura em tempo real, tornando o desempenho do produto mais estável, principalmente em máquinas com baixo desempenho de hardware.

**3.7.30** Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.

**3.7.31** Detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.

**3.7.32** Rastreamento manual com interface gráfica, customizável, com opção de limpeza.

**3.7.33** Rastreamento por linha de comando, parametrizável, com opção de limpeza.

**3.7.34** Programação de rastreamentos automáticos do sistema com as seguintes opções:

**e)** Escopo: todos os drives locais, específicos ou pastas específicas;

**f)** Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança;

**g)** Frequência: diária, semanal e mensal;

**h)** Exclusões: pastas ou arquivos que não devem ser rastreados;

**3.7.35** Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando.

**3.7.36** Detecção de anomalias através dos métodos de assinatura, heurística e por comportamento.

**3.7.37** Proteção contra ameaças via internet. A solução deve conter pelo menos:

**a)** Ajuste no nível de sensibilidade da detecção;

**b)** Lista de exceção.

**3.7.38** Detecção em tempo real e possibilidade de bloqueio e remoção de malwares provenientes de downloads realizados no ambiente web.

**3.7.39** Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser desabilitada;

**3.7.40** Detecção em tempo real e possibilidade de bloqueio e remoção de malwares no conteúdo e anexos de mensagens de correio eletrônico, pelo antivírus cliente, analisando tráfego e suportando principais clientes (no mínimo outlook).

**3.7.41** Permitir que a funcionalidade de rastreamento em tempo real de e-mail possa ser desabilitada.

**3.7.42** Detecção em tempo real e possibilidade de bloqueio e remoção de malwares nas áreas de armazenamento de dispositivos removíveis, tais como:

**n)** PenDrive;

**o)** HD externo;

**p)** Celulares;

**q)** Tablets;

**r)** CD/DVD;

**s)** Impressora USB;

**t)** Armazenamento de FireWire;

**u)** Dispositivo Bluetooth;

**v)** Leitor de cartão inteligente;

**w)** Dispositivo de criação de imagem;

**x)** Modem;

**y)** Porta LPT/COM;

**z)** Dispositivo portátil;

**3.7.43** O módulo de controle de dispositivos deve estar disponível para estações de trabalho Windows, macOS e Linux.

**3.7.44** Detecção, varredura, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação, nos formatos mais utilizados no mercado.

**3.7.45** Ferramenta de firewall bidirecional local no cliente, com possibilidade de configuração, ativação e desativação através da console de gerenciamento centralizada, contendo filtros especificados por aplicação, protocolo, IP, range de IPs, rede, porta e range de portas.

**3.7.46** A ferramenta de firewall local deverá tratar tráfego de entrada e de saída de forma independente.

**3.7.47** Deve permitir o bloqueio do “Autorun” nas portas USB ou bloquear automaticamente a execução de qualquer ameaça em dispositivos móveis.

**3.7.48** Permitir bloquear a conexão de dispositivos removíveis.

**3.7.49** Gerar registro (log) dos eventos de vírus em arquivo.

**3.7.50** Gerar relatórios, ao menos, de:

**d)** Eventos de vírus;

**e)** Status dos clientes;

**f)** Status dos Updates;

**3.7.51** Gerar notificações de eventos de vírus através de alerta por e-mail, ao menos.

**3.7.52** Gerar relatórios incluindo tipos de vírus, nome do vírus e se precisa de atualização do Sistema Operacional.

**3.7.53** 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.

**3.7.54** Permitir a criação de exceções nos escaneamentos de arquivos.

**3.7.55** Permitir o bloqueio de dispositivos com base nos seguintes critérios:

**d)** Fabricante;

**e)** Modelo;

**f)** Número de série;

**3.7.56** Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.

**3.7.57** A solução deve permitir a configuração de quais portas HTTPs serão escaneadas para verificação de conexões criptografadas.

**3.7.58** O Firewall deve possuir funcionalidade de suportar os protocolos TCP e UDP.

**3.7.59** O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.

**3.7.60** Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e Spoofing e botnet.

**3.7.61** Possibilidades de criação de assinaturas personalizadas para detecção.

**3.7.62** Possibilidade de agendar a ativação de novas regras do firewall.

**3.7.63** Possibilidade de criar regras diferenciadas por aplicações.

**3.7.64** Bloqueio de ataques baseado na exploração da vulnerabilidade.

**3.7.65** Permitir integração com navegadores WEB para prevenção de ataques.

**3.7.66** Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.

**3.7.67** Possuir taxa de performance de rede inferior a 70MB (megabytes) comprovada junto a instituições reconhecidas mundialmente em análises profundas de funcionalidades de fabricantes de soluções de segurança.

**3.7.68** A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.

**3.7.69** As configurações do antimalware deverão ser realizadas através do mesma console de todos os itens da solução.

**3.7.70** Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).

**3.7.71** Permitir verificação das ameaças de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do sistema operacional fornecendo a possibilidade de detecção de Rootkits.

**3.7.72** Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos, com intervalos de tempo determinados, de forma a reduzir impacto em ambientes.

**3.7.73** Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.

**3.7.74** Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP.

**3.7.75** Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos, mesmo que sejam compactados.

**3.7.76** Capacidade de terminar o processo e serviço da ameaça no momento de detecção.

**3.7.77** Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.

**3.7.78** Possibilidade de bloquear verificação de malware em recursos mapeados da rede.

**3.7.79** Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.

**3.7.80** Não serão aceitas soluções de Antimalware que possuam engine de terceiros.

**3.7.81** Permitir o bloqueio da execução de aplicações baseado em nome e pasta.

**3.7.82** A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações.

**3.7.83** Capacidade de detecção de keyloggers por comportamento dos processos em memória.

**3.7.84** Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts.

**3.7.85** Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.

**3.7.86** Realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como:

**f)** Aprendizado de máquina;

**g)** Deep Learning;

**h)** Análise estatística e dinâmica;

**i)** Detecção baseada em comportamento;

**j)** Introspecção na memória;

**3.7.87** Detecção do malware por DNA do vírus.

**3.7.88** Deverá ter a capacidade de atualizar os patches do sistema operacional.

**3.7.89** A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hypervisor.

**3.7.90** Em servidores que usam “OneDrive for Business” deve ser possível explorar os arquivos armazenados nesta nuvem, procurando por arquivos comprometidos ou possível malware.

**3.7.91** A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços que foram identificados com este comportamento malicioso.

**3.7.92** A solução deve adicionar exclusões automaticamente para aplicativos de servidor críticos.

**3.7.93** A solução deve possuir otimização de desempenho para infraestruturas mistas (física e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.

**3.7.94** Controlar acesso a sites, possibilitando o bloqueio dos mesmos.

**3.7.95** Permitir criar políticas de bloqueio com base em categorias e lista de URL.

**3.7.96** Permitir gerar relatórios de sites acessados e bloqueados.

**3.7.97** Permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.

**3.7.98** Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.

**3.7.99** Para o módulo de proteção de e-mail, deve suportar minimamente os seguintes protocolos:

**e)** POP3;

**f)** POP3S;

**g)** IMAP;

**h)** IMAPS;

**3.7.100** Deve permitir a configuração de ações personalizadas para detecções realizadas pelo módulo de proteção de e-mail, suportando minimamente as seguintes ações:

**d)** Mover o e-mail para uma pasta;

**e)** Excluir o e-mail;

**f)** Manter o e-mail;

**3.7.101** Em equipamentos macOS, a solução deve possuir módulo para proteção de e-mails de entrada e saída.

**3.7.102** Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.

**3.7.103** A solução de proteção antispam deve realizar as verificações utilizando o protocolo SSL.

**3.7.104** O módulo de proteção antispam deverá ser nativo e integrado ao Endpoint.

**3.7.105** Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push.

**3.8 Solução de Sandbox em nuvem**

**3.8.1** Deve ser possível criar exclusões por caminho, nome de detecção e hash do arquivo (SHA-1).

**3.8.2** A solução deve permitir a definição do tempo máximo para análise automática de artefatos.

**3.8.3** Capacidade de sincronizar seu licenciamento com a nuvem e o console de administração no local (on-premise) ou na nuvem.

**3.8.4** Detectar um arquivo suspeito executado pela primeira vez, um aviso deve ser exibido, se a verificação for concluída antes do arquivo ser executado pela primeira vez, o aviso de arquivo sob verificação não será exibido. Deve eliminar automaticamente as amostras dos arquivos/executáveis nos servidores onde o comportamento foi analisado.

**3.8.5** Capacidade para enviar e-mails de SPAM para sua análise.

**3.8.6** Deve classificar os artefatos em categorias, oferecendo no mínimo as seguintes categorias: desconhecido, limpo, suspeito, altamente suspeito e malicioso.

**3.8.7** Deve disponibilizar as seguintes informações de um arquivo enviado ao Sandbox na nuvem: nome do equipamento que enviou o arquivo, o usuário conectado no dispositivo, o resultado da análise, hash no formato SHA-1, nome do arquivo analisado, tamanho do arquivo, categoria.

**3.8.8** Deve oferecer proteção proativa, ou seja, que o arquivo/executável seja bloqueado até receber o resultado do Sandbox na nuvem.

**3.8.9** A solução deve possuir integração com a solução de antimalware, para possuir maiores possibilidades de proteção e aplicação de políticas.

**3.8.10** A solução de Sandbox em nuvem deve estar disponível minimamente para integração com os produtos para estações e servidores Windows e Linux.

**3.8.11** Deve ser possível enviar um arquivo/executável manualmente para a solução de Sandbox em nuvem.

**3.9 Solução para criptografia de discos**

**3.9.1** A solução deverá ser capaz de criptografar dispositivos Windows e macOS.

**3.9.2** Para estações Windows, a solução deverá possuir tecnologia própria de criptografia. Não serão aceitas soluções que apenas oferecem gerenciamento do BitLocker (Microsoft).

**3.9.3** Para estações macOS, a solução deve ser capaz de gerenciar o FileVault, disponibilizado pela Apple.

**3.9.4** A solução deverá ser capaz de criptografar os Endpoints desejados desde o início do sistema operacional.

**3.9.5** A solução deverá dispor de diversas possibilidades de recuperação de senha para usuários remotos que estejam bloqueados.

**3.9.6** A solução deverá poder programar as tarefas de criptografia sobre os Endpoints desejados com a possibilidade de pausar a execução para retomar desde o último estado.

**3.9.7** A solução deverá ser administrada desde o mesmo console central junto com as outras soluções descritas neste termo de referência.

**3.9.8** Possibilitar a opção de criptografar apenas o disco de inicialização.

**3.9.9** Possibilitar que as estações de trabalho sejam criptografas sem que o recurso de TPM (Trusted Platform Module) esteja válido.

**3.9.10** Através da console central deve ser possível invalidar a senha de login do usuário e solicitar que mude sua senha de login por meio de uma interface gráfica.

**3.9.11** Deve possibilitar que o administrador recupere os dados caso o usuário não consiga acessar a máquina com suas credenciais.

**3.9.12** Deve possibilitar que o administrador gere uma nova senha de recuperação para o usuário.

**3.10 Outros requerimentos gerais**.

**3.10.1** A solução ofertada não deve possuir restrições sobre a quantidade de equipamentos para ativação das licenças. A totalidade das licenças contratadas pode ser ativada completamente em servidores, estações de trabalho, ou dispositivos móveis, respeitando o limite total contratado.

**3.10.2** Todos os módulos ofertados pelo fabricante, devem ser ativados utilizando uma única licença, sem a necessidade de aquisição de módulos separados (add-ons).

**3.10.3** O fabricante deve comprovar premiações e participações em programas de certificação.

**3.10.4** O fabricante deverá ter suporte local em idioma português.

**3.10.5** O fabricante deve oferecer serviços de segurança da informação como por exemplo: teste de penetração, avaliação de vulnerabilidade ou análise de GAPs.

**3.10.6** O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.

**3.10.7** O fabricante deve possuir escritório próprio no Brasil.

**3.10.8** Possuir manuais de apoio sobre a solução em português.

**3.10.9** O fabricante deverá ter documentação publicada na internet no idioma português.

**3.10.10** O fabricante deve contar com a certificação de segurança ISO 27001.

**Da Compatibilidade com Sistemas Legados:**

**b)** A operacionalidade da Solução em Sistemas Legados (por exemplo: Windows 7, 8.1) será garantida pelo uso de *engines* de versões anteriores buscando, se possível, o gerenciamento único.

## (04) Prazo, local e condições de entrega ou execução

### 4.1 Prazo e local

**4.1.1** O início da vigência das licenças deverá ser a partir de **23/11/2024**, devido ao encerramento do contrato atual, portanto nesta data as licenças deverão estar devidamente instaladas e em pleno funcionamento.

**4.1.2 O prazo de execução será de 60 meses.**

### 4.2 Instalação

**4.2.1** As licenças deverão ser entregues e os softwares instalados de acordo com as orientações da equipe técnica do CONTRATANTE, nos endereços das diversas unidades da UNITAU.

**4.2.2** Caso seja possível, a CONTRATADA poderá fazer a instalação dos softwares nas unidades através da rede de dados da UNITAU, mas presencialmente na Central de TI;

**4.2.3** A CONTRATADA deverá elaborar e apresentar para aprovação um Projeto de Instalação do software, envolvendo:

**4.2.3.1** Desinstalação do software de segurança instalado atualmente nas estações e servidores de arquivos da UNITAU;

**4.2.3.2** Instalação do novo software, sem prejuízo da operação da rede atual e minimizando o risco de infecção por não existência de antivírus nas estações;

**4.2.3.3** Criação de perfis de usuários no software de gerenciamento;

**4.2.3.4** Criação de regras e grupos de acordo com as diretrizes da equipe técnica do CONTRATANTE;

**4.2.3.5** Testes de aceite e comprovação de funcionamento;

**4.2.3.6** Passagem de conhecimento para a equipe técnica do CONTRATANTE.

**4.2.4** A CONTRATADA deverá fornecer a documentação de todo o projeto;

**4.2.4.1** A instalação do software deverá ser efetuada pela CONTRATADA, conforme orientação da Central de Tecnologia da Informação – CeTI da CONTRATANTE.

**4.2.4.2** A entrega e instalação seguirá o seguinte cronograma:

| Etapa | Intervalo (dias úteis) | Descrição |
|---|---|---|
| 1 | 1 | Emissão da Autorização do Início dos Serviços |
| 2 | 15 | Entrega das licenças de softwares e do cronograma de instalação conforme item 4 deste Termo de Referência. |
| 3 | 30 | Instalação e configuração dos softwares da solução, incluindo desinstalações de softwares anteriores, se for o caso. |
| 4 | 15 | Operação Assistida de Funcionamento da Solução. |
| 5 | 10 | Treinamento com duração mínima de 20 horas |

**4.2.4.3** A operação assistida, citada na etapa 4 da tabela acima, consiste na permanência na UNITAU de um profissional da CONTRATADA para atender e solucionar todas as dúvidas e problemas que possam ocorrer com a solução.

**4.2.4.3.1** O horário de permanência do profissional responsável citado no item 4.2.4.3 deverá ser o mesmo do expediente da Contratante, de segunda-feira à sexta-feira, das 8h às 12h e das 14h às 18h.

**4.2.4.4** A CONTRATANTE expedirá os atestados de aceite técnico das etapas de entrega da solução, em até 5 dias da comunicação formal da CONTRATADA, de que a solução encontra-se devidamente instalada, ou das conclusões das etapas, após as devidas verificações.

**4.2.4.5** O CONTRATANTE deverá fornecer as mídias para instalação dos softwares.

### 4.3 Treinamento

**4.3.1** Fornecer treinamento presencial ou on-line, em português, com interação entre as partes, para 6 (seis) servidores da UNITAU e treinamentos contínuos online em plataforma web própria tanto da solução adquirida, quanto das demais soluções para ampliação de conhecimentos técnicos.

**4.3.2** Os treinamentos serão aceitos de forma on-line desde que a Contratada, ofereça ferramentas e ambientes para simulação e configuração conforme a estrutura verificada no momento da instalação na UNITAU. Além disso, os treinamentos e/ou reuniões on-line deverão ser gravados e disponibilizados para consultas posteriores.

**4.3.3** Os custos com transporte, alimentação e estadia deverão correr por conta da CONTRATADA.

**(05) Prazos e condições de garantia**

Não se aplica

**(06) Responsável pelo recebimento**

**Nome:** Jaqueline Blanco

**Cargo:** Coordenadora da Central de Tecnologia da Informação

**Setor:** Central de Tecnologia da Informação

**Endereço:** Rua Expedicionário Ernesto Pereira, 116, Centro, Taubaté, SP, CEP 12020-330

**Telefone:** 12 3625-4111

**E-mail:** infra@unitau.br

**(07) Condições e prazos de pagamento**

O pagamento será realizado em até 21 (vinte e um) dias após ateste definitivo da Nota Fiscal pelo responsável técnico.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**(08) Obrigações da contratada**

**I.** Manter, durante todo o prazo de vigência deste Contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de qualificação e habilitação exigidas;

**II.** Não utilizar quaisquer informações às quais tenha acesso, em virtude desta contratação, em benefício próprio ou em trabalhos de qualquer natureza, nem divulgá-las sem autorização por escrito da CONTRATANTE;

**III.** Conduzir a execução da presente avença de acordo com o Termo de Referência e Proposta Comercial e de conformidade com as normas técnicas aplicáveis, observando estritamente a legislação vigente aplicável;

**IV.** Arcar com todos os ônus ou obrigações decorrentes da legislação da seguridade social, trabalhista, tributária, fiscal, securitária, comercial, civil e criminal, no que se relacionem com a execução do objeto desta avença, inclusive no tocante a seus empregados, dirigentes e prepostos;

**V.** Responder, por si e por seus sucessores, integralmente e em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados à CONTRATANTE ou a terceiros, por seus empregados ou serviços, indenizando quando for necessário;

**VI.** Substituir, a suas expensas e responsabilidade, na forma da lei, os produtos que não estiverem de acordo com as especificações;

**VII.** A CONTRATADA realizará a instalação do Software conforme item 4 (quatro) deste Termo;

**VIII.** Disponibilização de treinamento presencial ou on-line, em português, com interação entre as partes, para 6 (seis) servidores da UNITAU e treinamentos contínuos online em plataforma web própria tanto da solução adquirida, quanto das demais soluções para ampliação de conhecimentos técnicos.

**IX.** Os treinamentos serão aceitos de forma on-line desde que a Contratada, ofereça ferramentas e ambientes para simulação e configuração conforme a estrutura verificada no momento da instalação na UNITAU. Além disso, os treinamentos e/ou reuniões on-line deverão ser gravados e disponibilizados para consultas posteriores.

**(09) Obrigações da contratante**

**I.** Assegurar à CONTRATADA o recebimento dos créditos decorrentes do adimplemento de suas obrigações, acompanhada da atualização monetária entre a data do adimplemento e a do efetivo pagamento, com a aplicação do índice INPC/IBGE, se for o caso;

**II.** Permitir à CONTRATADA o livre acesso às dependências relacionadas a execução do objeto desta avença, em horários previamente estabelecidos;

**III.** Fiscalizar a execução do ajuste e documentar as ocorrências havidas em registro próprio;

**IV.** Assegurar o recebimento dos créditos decorrentes do adimplemento de suas obrigações, acompanhada da atualização monetária entre a data do adimplemento e a do efetivo pagamento, com a aplicação do índice INPC/IBGE, se for o caso;

**V.** Fiscalizar instalação e atualização do Software.

## (10) Qualificação técnica

**I.** Atestado(s) emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, em nome do licitante, em pelo menos 50% da quantidade do Lote.

**II.** O(s) atestado(s) deverá(ão) conter: prazo contratual e datas de início e término; local da prestação dos serviços; natureza da prestação dos serviços; quantidades executadas; caracterização do bom desempenho do licitante; outros dados característicos; e a identificação da pessoa jurídica emitente bem como o nome e o cargo do signatário.

**III.** A referida comprovação poderá ser efetuada pelo somatório das quantidades realizadas em tantos contratos quanto dispuser o licitante.

**IV.** O(s) documento(s) deve(m) conter a razão social, CNPJ, o nome e assinatura do representante legal, o endereço e o telefone de contato do(s) atestado(res), ou qualquer outra forma de que a Universidade de Taubaté possa valer-se para manter contato com a(s) empresa(s) declarante(s).

**V.** O Atestado de Capacidade Técnica deverá comprovar o fornecimento, instalação, treinamento, manutenção e suporte na solução ofertada.

**VI.** Declaração emitida pelo Fabricante que a Solução oferecida atende na sua última versão a todos os Quesitos Técnicos exigidos no Item 3.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**(11) Critério de avaliação das propostas**

O critério será o de Menor Preço Total do Item.

**(12) Resultados esperados**

Garantir o acesso, a segurança e a propriedade dos dados, sistemas e equipamentos de propriedade ou sob custódia das áreas de negócio da Universidade de Taubaté.

**(13) Sanções**

**13.1.** Pela inexecução total ou parcial do objeto contratado, deixar de entregar documentação exigida, não manter a proposta, erro de execução, execução imperfeita, retardamento da execução ou da entrega do objeto, inadimplemento contratual ou ainda comportar-se de modo inidôneo, cometer fraude de qualquer natureza ou constatar-se a não veracidade de informações prestadas à Administração, praticar atos ilícitos e lesivos, poderá a Administração aplicar a Licitante ou a Contratada, garantida a prévia e ampla defesa, nos termos do Art. 155, da Lei Federal nº 14.133/21, as sanções administrativas que seguem:

**a)** advertência por escrito por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos ao objeto contratado, sendo exigida pronta reparação da falta cometida e comunicação formal das providências tomadas;

**b)** multa de 2% (dois por cento), sobre o valor total do contrato, por reincidência de 02 (duas) advertências;

**c)** multa equivalente a 4% (quatro por cento), sobre o valor total do contrato, por dia, pelo não cumprimento dos prazos de entrega, admitindo-se o máximo de 05 (cinco) dias, após o que poderá ser reconhecida a inexecução do ajuste;

**d)** multa de 10% (dez por cento), sobre o valor total do contrato, por infração a qualquer condição do contrato e, aplicada em dobro, em caso de reincidência;

**e)** multa de 20% (vinte por cento), sobre o valor total do contrato, por inexecução parcial deste ajuste, observando-se a proporcionalidade de

parte do contrato cumprido, independentemente das demais sanções cabíveis;

**f)** multa de 30% (trinta por cento), sobre o valor total do contrato, por inexecução total deste juste, independentemente das demais sanções cabíveis;

**g)** multa de 30% (trinta por cento), sobre o valor total homologado, pela recusa injustificada da licitante vencedora em assinar o Contrato;

**h)** no caso de reincidência em irregularidades na execução do objeto por 03 (três) vezes, poderá considerar caracterizada a inexecução do objeto e rescindir o ajuste, sem prejuízo das multas estipuladas nas alíneas anteriores;

**i)** impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo, por prazo de 03 (três) anos, nos casos descritos nos incisos III, IV, V e VI do caput do art. 155 da Lei Federal 14.133/2021, e por prazo de 02 (dois) anos, nos casos descritos nos incisos II, VII do caput do art. 155, da Lei Federal 14.133/2021, admitindo-se a sua reabilitação nos termos do Art. 163, da mesma lei.

**j)** declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, por prazo de 06 (seis) anos, nos casos descritos nos incisos VIII, IX, X, XI e XII do caput do art. 155 da Lei Federal 14.133/2021, admitindo-se a sua reabilitação nos termos do Art. 163, da mesma lei.

**13.2.** As multas deverão ser recolhidas, por depósito bancário identificado, na conta corrente nº 45.000045-5, agência 0056, Banco Santander, em nome da Universidade de Taubaté, no prazo de até 15 (quinze) dias úteis, contado da data de sua intimação.

**13.2.1.** O comprovante de depósito deverá ser encaminhado, no prazo acima, ao e-mail do setor responsável pela intimação.

**13.3.** Se o valor da multa aplicada e as indenizações cabíveis não forem pagos, os mesmos deverão ser descontados dos pagamentos eventualmente devidos à Administração, ou descontados da garantia prestada ou será cobrada judicialmente.

**13.4.** A aplicação das penalidades não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

**13.5.** Para as penalidades previstas, será garantido o direito ao contraditório e à ampla defesa, a qual deverá ser apresentada pelo interessado no prazo de 15 (quinze) dias úteis, contado da data de sua notificação, que será dirigida para análise da Douta Procuradoria Jurídica;

**13.6.** As sanções serão obrigatoriamente registradas em autos próprios, e no caso da aplicação do impedimento de licitar e contratar e da declaração de inidoneidade, requererá a instauração de processo de responsabilização, a ser conduzido por comissão, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir, nos termos do Art. 158, da Lei Federal 14.133/21.

**13.7.** As penalidades só poderão ser relevadas nas hipóteses de caso fortuito ou força maior, devidamente justificada e comprovada, a juízo da Administração.

## (14) Estimativas do valor da Contratação

As estimativas estão discriminadas no item 8 do Estudo Técnico Preliminar – ETP CETI nº 10/2024.

**A estimativa atualizada, constará em anexo neste Termo de Referência,** após pesquisa de preços a ser realizada pelo Serviço de Licitações e Compras, conforme parâmetros estabelecidos nos incisos I, II, III, IV e V, do §1º, artigo 23, da Lei Federal nº 14.133/2021 e validação pelo responsável do Setor requisitante.

## (15) Adequação Orçamentária

As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Universidade de Taubaté.

A contratação será atendida pela seguinte dotação: 12.122.0104.4003.339040.

## (16) Condições gerais

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

Não se aplica.

## (17) Matriz de Risco

Não se aplica.

**Jaqueline Blanco**
**Coordenadora da Central de Tecnologia da Informação**

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# ANEXO A

# PESQUISA DE MERCADO ATUALIZADA

**UNIVERSIDADE DE TAUBATE - UNITAU - SP**

***Pedido de Orçamento - Mapa Comparativo***

**Ano: 2024** **Número: 146**
**Comprador: 638331 - GEORGIA LUIZE VARGAS SILVA**
**Descrição: 1295**

| Seq | Grupo Material | Item | Qtde | U.M. | Valor Médio | Maior Valor | Menor Valor |
|---|---|---|---|---|---|---|---|
| Descrição/Desc. Complementar | | | | | | | |
| Fornecedor | | | Cotação | Valor Total | Marca | | Prazo Entr. |
| 1 | 18 | 0180010082 | 2.000,0000 | LIC | 234,83 | 290,00 | 204,50 |
| SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, CONFORME ES | | | | | | | |
| TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO | | | 204,5000 | 409.000,00 | | | 365 - Dias |
| COMANDO DO EXERCITO | | | 210,0000 | 420.000,00 | | | 365 - Dias |
| MUNICIPIO DE SAQUAREMA | | | 290,0000 | 580.000,00 | | | 365 - Dias |

| VALOR TOTAL | |
|---|---|
| **Médio:** | 469.660,00 |
| **Maior:** | 580.000,00 |
| **Menor:** | 409.000,00 |



# ANEXO VI

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

# MINUTA DE CONTRATO

**Processo:** PRA – 343/2024

**Licitação:** Pregão Eletrônico nº 27/24

**Regência Legal:** Lei Federal nº Lei Federal nº 14.133/21, Lei Complementar nº 123/06 e suas alterações e pelo Decreto Municipal de Taubaté n° 15.447/22.

**Objeto:** Aquisição de solução de segurança corporativa para endpoints, servidores e rede UNITAU conforme especificações deste termo de referência, comtemplando suporte presencial/remoto para instalação, configuração, customização e treinamento, por 60 meses

**Valor:** R$ 469.660,00

**Vigência:** 60 (SESSENTA) meses

Pelo presente instrumento, de um lado, na qualidade de CONTRATANTE, a **UNIVERSIDADE DE TAUBATÉ**, inscrita no CNPJ sob o nº 45.176.153/0001-22, neste ato, representada por _____, à Rua Quatro de Março nº 432, Centro, Taubaté/SP, e, de outro lado, na qualidade de CONTRATADA a empresa _____, com sede à _____, inscrita no CNPJ sob nº _____, com Inscrição Estadual nº _____, Inscrição Municipal nº _____, com contrato social arquivado na Junta Comercial do Estado de _____ sob NIRE _____, neste ato, representada pelo _____, portador do RG nº _____, inscrito no CPF sob nº _____, representante legal da adjudicatária do objeto do PREGÃO ELETRÔNICO nº 27, de que trata o Processo PRA nº 343/2024, homologado pela Pró-Reitoria de Administração, publicada na Imprensa Oficial aos _____, têm entre si justo e contratado, nos termos do que determinam a Lei Federal nº 14.133/21, Lei Complementar nº 123/06 e suas alterações e pelos Decreto Municipal de Taubaté n° 15.447/22 e obedecidas às disposições contidas no Edital e seus Anexos, os quais se vinculam ao presente termo, o que se segue:

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**CLÁUSULA PRIMEIRA - DO OBJETO**

A CONTRATADA, na qualidade de adjudicatária do PREGÃO ELETRÔNICO 27/24, de que trata o Processo PRA nº 343/2024 obriga-se a cumprir o estabelecido neste instrumento contratual, que tem por objeto SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, tudo em conformidade com as descrições, especificações e demais disposições constantes do Edital e seus anexos, aos quais se vincula o presente instrumento de contrato, para todos os efeitos.

PARÁGRAFO ÚNICO – O(s) Item(s) a ser(em) fornecido(s) pela CONTRATADA apresenta(m) o seguinte conteúdo:

| Item | Descritivo | Quant. | Unid. | Valor Unitário | Valor Total |
|---|---|---|---|---|---|
| 01 | SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS | 2.000 | LICENÇA | **234,83** | **469.660,00** |

**CLÁUSULA SEGUNDA - DA EXECUÇÃO DO OBJETO**

2.1. O prazo de início da vigência das licenças será à partir de 23/11/2024.

2.2. As licenças deverão ser encaminhadas para o e-mail infra@unitau.br e a execução do objeto deverá ocorrer conforme estabelecido no Anexo V – Termo de Referência.

**CLÁUSULA TERCEIRA - DO PREÇO, DO ELEMENTO ECONÔMICO E DAS CONDIÇÕES DE PAGAMENTO**

3.1. O preço total do objeto enunciado na Cláusula Primeira deste ajuste, nos termos da Proposta Comercial, e da Ata do Pregoeiro é de R$ 469.660,00 (quatrocentos e sessenta e nove mil seiscentos e sessenta reais), correndo por conta das Notas de Empenho nº 550/2024 que oneram a dotação orçamentária nº 1212201044003 e nº _____ do exercício financeiro de 2024.

3.2. A CONTRATANTE efetuará o pagamento da contraprestação à CONTRATADA em até 21 (vinte e um) dias, contados da data do Ateste no verso da Nota Fiscal/Fatura, pelo responsável da unidade requisitante, que deverá ser apresentada juntamente com os documentos de cobrança, sem qualquer correção monetária, de acordo com o Termo de Referência, Anexo V, do Edital.

§1º - O requerimento de pagamento, bem como os documentos de cobrança da CONTRATADA, deverão ser entregues juntamente com a Nota Fiscal/Fatura na Central de Tecnologia da Informação da UNITAU, telefone: (12) 3625-4111, e-mail: infra@unitau.br.

§ 2º - Caso o dia do pagamento recaia em dia não útil, esse será efetuado no primeiro dia útil subsequente, sendo certo que, mesmo nesse caso, manter-se-á, na fatura, o dia do vencimento.

§ 3º - As Notas Fiscais/Faturas que apresentarem incorreções serão devolvidas à CONTRATADA para as devidas correções. Nesse caso, o prazo de que trata o parágrafo primeiro desta cláusula começará a fluir a partir da data de reapresentação da nota fiscal/fatura corrigida.

§ 4º - Em atenção à Instrução Normativa RFB nº 2145, de 26/06/2023, informamos que é **obrigatório** destacar o valor e a alíquota do IR a ser retido **no corpo da Nota Fiscal**. Caso o fornecedor seja isento ou imune, uma declaração deverá ser apresentada.

**CLÁUSULA QUARTA - DA GARANTIA**

4.1. Durante o prazo de garantia dos produtos fornecidos, como disposto em legislação vigente e estabelecido na Proposta Comercial, sendo constatados vícios de qualidade dos serviços, que tornem inadequada sua utilização, poderá a CONTRATANTE, sem prejuízo da aplicação das penalidades previstas na Lei Federal nº 14.133/21, exigir, alternativamente e à sua escolha, o seguinte:

a) o atendimento ao chamado em 24 horas e solução em 72 horas para sanar o problema detectado, sem ônus à CONTRATANTE;

b) a restituição imediata da quantia paga, monetariamente atualizada, se for o caso, relativa ao(s) serviço(s) que apresentar(em) vício(s) de qualidade, conforme inspeção realizada pelo responsável da unidade requisitante da UNITAU, sem prejuízo de eventuais perdas e danos, no prazo de 10 (dez) dias, contado da solicitação

**CLÁUSULA QUINTA - DOS ENCARGOS**

Os encargos trabalhistas, previdenciários, fiscais, comerciais, de transportes e seguro, inclusive aqueles relativos a impostos e taxas, são de inteira responsabilidade da CONTRATADA, bem como despesas e obrigações financeiras de qualquer natureza, despesas operacionais, mão-de-obra, inclusive horas extras e

adicionais noturnos de profissionais, auxílio alimentação, auxílio transporte e transporte local, sendo que sua inadimplência, com relação a tais encargos, não transfere à CONTRATANTE o ônus pelo seu pagamento, não podendo onerar a presente avença.

**CLÁUSULA SEXTA - DAS OBRIGAÇÕES DA CONTRATADA**

São obrigações da CONTRATADA, além de outras fixadas no **ANEXO V – TERMO DE REFERÊNCIA** e no Edital, as seguintes:

I - manter, durante todo o prazo de vigência deste Contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de qualificação e habilitação exigidas no respectivo procedimento licitatório;

II - não utilizar quaisquer informações às quais tenha acesso, em virtude deste Contrato, em benefício próprio ou em trabalhos de qualquer natureza, nem divulgá-las sem autorização por escrito da CONTRATANTE;

III - conduzir a execução da presente avença de acordo com o Anexo I e Proposta Comercial e de conformidade com as normas técnicas aplicáveis, observando estritamente a legislação vigente aplicável;

IV - arcar com todos os ônus ou obrigações decorrentes da legislação da seguridade social, trabalhista, tributária, fiscal, securitária, comercial, civil e criminal, no que se relacionem com a execução do objeto desta avença, inclusive no tocante a seus empregados, dirigentes e prepostos;

V - responder, por si e por seus sucessores, integralmente e em qualquer caso, por todos os danos e prejuízos, de qualquer natureza, causados à CONTRATANTE ou a terceiros, por seus empregados ou serviços, indenizando quando for necessário;

VI - substituir, a suas expensas e responsabilidade, na forma da lei, os produtos que não estiverem de acordo com as especificações;

VII - não divulgar quaisquer dados, conhecimentos e resultados decorrentes da execução do objeto deste Contrato, sem prévia e expressa autorização da CONTRATANTE;

**CLÁUSULA SÉTIMA - DAS OBRIGAÇÕES DA CONTRATANTE**

São obrigações da CONTRATANTE, além de outras fixadas no **ANEXO V– TERMO DE REFERÊNCIA** e no Edital, as seguintes:

I - assegurar à CONTRATADA o recebimento dos créditos decorrentes do adimplemento de suas obrigações, acompanhada da atualização monetária entre a data do adimplemento e a do efetivo pagamento, com a aplicação do índice INPC/IBGE, se for o caso;

II - permitir à CONTRATADA o livre acesso às dependências relacionadas a execução do objeto desta avença, em horários previamente estabelecidos;

III - fornecer todas as informações, esclarecimentos e as condições necessárias à plena execução do objeto do presente ajuste;

**CLÁUSULA OITAVA - DAS PENALIDADES E DAS MULTAS**

8.1. Pela inexecução total ou parcial do objeto contratado, deixar de entregar documentação exigida, não manter a proposta, erro de execução, execução imperfeita, retardamento da execução ou da entrega do objeto, inadimplemento contratual ou ainda comportar-se de modo inidôneo, cometer fraude de qualquer natureza ou constatar-se a não veracidade de informações prestadas à Administração, praticar atos ilícitos e lesivos, poderá a Administração aplicar a Licitante ou a Contratada, garantida a prévia e ampla defesa, nos termos do Art. 155, da Lei Federal nº 14.133/21, as sanções administrativas que seguem:

a) advertência por escrito por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos ao objeto contratado, sendo exigida pronta reparação da falta cometida e comunicação formal das providências tomadas;

b) multa de 2% (dois por cento), sobre o valor total do contrato, por reincidência de 02 (duas) advertências;

c) multa equivalente a 4% (quatro por cento), sobre o valor total do contrato, por dia, pelo não cumprimento dos prazos de entrega, admitindo-se o máximo de 05 (cinco) dias, após o que poderá ser reconhecida a inexecução do ajuste;

d) multa de 10% (dez por cento), sobre o valor total do contrato, por infração a qualquer condição do contrato e, aplicada em dobro, em caso de reincidência;

e) multa de 20% (vinte por cento), sobre o valor total do contrato, por inexecução parcial deste ajuste, observando-se a proporcionalidade de parte do contrato cumprido, independentemente das demais sanções cabíveis;

f) multa de 30% (trinta por cento), sobre o valor total do contrato, por inexecução total deste juste, independentemente das demais sanções cabíveis;

g) multa de 30% (trinta por cento), sobre o valor total homologado, pela recusa injustificada da licitante vencedora em assinar o Contrato;

h) no caso de reincidência em irregularidades na execução do objeto por 03 (três) vezes, poderá considerar caracterizada a inexecução do objeto e rescindir o ajuste, sem prejuízo das multas estipuladas nas alíneas anteriores;
i) impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo, por prazo de 03 (três) anos, nos casos descritos nos incisos III, IV, V e VI do caput do art. 155 da Lei Federal 14.133/2021, e por prazo de 02 (dois) anos, nos casos descritos nos incisos II, VII do caput do art. 155, da Lei Federal 14.133/2021, admitindo-se a sua reabilitação nos termos do Art. 163, da mesma lei.

j) declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, por prazo de 06 (seis) anos, nos casos descritos nos incisos VIII, IX, X, XI e XII do caput do art. 155 da Lei Federal 14.133/2021, admitindo-se a sua reabilitação nos termos do Art. 163, da mesma lei.

8.2. As multas deverão ser recolhidas, por depósito bancário identificado, na conta corrente nº 45.000045-5, agência 0056, Banco Santander, em nome da Universidade de Taubaté, no prazo de até 15 (quinze) dias úteis, contado da data de sua intimação.

8.2.1. O comprovante de depósito deverá ser encaminhado, no prazo acima, ao e-mail do setor responsável pela intimação.

8.3. Se o valor da multa aplicada e as indenizações cabíveis não forem pagos, os mesmos deverão ser descontados dos pagamentos eventualmente devidos à Administração, ou descontados da garantia prestada ou será cobrada judicialmente.

8.4. A aplicação das penalidades não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

8.5. Para as penalidades previstas, será garantido o direito ao contraditório e à ampla defesa, a qual deverá ser apresentada pelo interessado no prazo de 15 (quinze) dias úteis, contado da data de sua notificação, que será dirigida para análise da Douta Procuradoria Jurídica;

8.6. As sanções serão obrigatoriamente registradas em autos próprios, e no caso da aplicação do impedimento de licitar e contratar e da declaração de inidoneidade, requererá a instauração de processo de responsabilização, a ser conduzido por comissão, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir, nos termos do Art. 158, da Lei Federal 14.133/21.

8.7. As penalidades só poderão ser relevadas nas hipóteses de caso fortuito ou força maior, devidamente justificada e comprovada, a juízo da Administração.

O presente contrato poderá ser rescindido nas hipóteses previstas na Lei Federal nº 14.133/21, sem prejuízo das sanções previstas neste ajuste.

§1º - A prática do disposto no artigo 137, da Lei Federal nº 14.133/21, pela CONTRATADA, poderá determinar a rescisão contratual, por ato unilateral da CONTRATANTE, sem prejuízo das sanções previstas na referida lei, exceto, na hipótese de associação da CONTRATADA com outrem, fusão cisão ou incorporação, desde que tal fato não acarrete prejuízo para a execução do contrato.

§2º - Ocorrendo a rescisão, nos termos da Lei Federal nº 14.133/21, sem culpa da CONTRATADA, será esta ressarcida dos prejuízos que comprovadamente houver sofrido.

§3º - No que se refere ao inciso I do artigo 137, da Lei Federal nº 14.133/21, não constitui motivo para rescisão contratual, tampouco indenização à CONTRATADA, a hipótese em que houver supressão do objeto contratado, além dos limites estabelecidos em lei, resultante de acordo celebrado entre as partes, segundo permissivo legal disposto no artigo 125, da Lei Federal nº 14.133/21.

§4º - À CONTRATANTE é reconhecido o direito de rescisão administrativa, nos termos do artigo 138, III, da Lei Federal nº 14.133/21, aplicando-se no que couber o disposto nos §§1º e 2º do citado artigo, bem como as regras do artigo 139 do mesmo diploma legal.

**CLÁUSULA DÉCIMA - DA IMPOSSIBILIDADE DE SUBCONTRATAÇÃO**

A CONTRATADA não poderá subcontratar no todo ou parte o objeto de que trata a Cláusula Primeira.

**CLÁUSULA DÉCIMA PRIMEIRA - DAS ALTERAÇÕES CONTRATUAIS**

Qualquer alteração contratual deverá observar o disposto no artigo 124, da Lei Federal nº 14.133/21

**CLÁUSULA DÉCIMA SEGUNDA - DA LEGISLAÇÃO APLICADA**

A execução deste contrato será disciplinada pela Lei Federal nº 14.133/21, sendo regulada por suas cláusulas e preceitos de direito público, aplicando-se-lhe, supletivamente, os princípios de teoria geral dos contratos e as disposições de direito privado.

**CLÁUSULA DÉCIMA TERCEIRA - DA VIGÊNCIA**

13.1. O prazo de vigência deste instrumento será de **60 (sessenta) meses**, contado a partir de 23/11/2024.

13.2. Após o primeiro ano de contratação, o valor pactuado poderá ser reajustado mediante aplicação do índice INPC/IBGE, acumulado do mês anterior ao vencimento.

**CLÁUSULA DÉCIMA QUARTA - DA FISCALIZAÇÃO**

A execução do presente Contrato será acompanhada e fiscalizada pelo setor requisitante, da CONTRATANTE, a qual anotará em registro próprio qualquer ocorrência havida que esteja em desacordo com os termos da proposta comercial ou deste instrumento contratual, determinando, em decorrência disto, o que for necessário à regularização das falhas observadas.

14.1. A execução do objeto será acompanhada pela servidora Jaqueline Blanco, e-mail: infra@unitau.br; telefone (12) 3625-4111.

14.2. A fiscalização da execução do objeto pela CONTRATANTE não exclui nem reduz a responsabilidade da CONTRATADA pela inobservância de qualquer obrigação assumida.

**CLÁUSULA DÉCIMA QUARTA - DECLARAÇÕES E GARANTIAS ANTI CORRUPÇÃO**

14.1. Nenhuma das partes, por si e por seus administradores, diretores, empregados, associados, agentes, proprietários e/ou acionistas, que atuam em seu nome ou estão envolvidos no dia-a-dia de suas operações, poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer país, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma que não relacionada a este contrato, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

14.2. As partes declaram neste ato que estão cientes, conhecem e entendem os termos das leis anticorrupção brasileiras, em especial aquelas estabelecidas na Lei nº 12.846 de 01 de agosto de 2.013 ou de quaisquer outras aplicáveis sobre o objeto do presente contrato, comprometendo-se a abster-se de qualquer atividade que constitua uma violação das disposições destas Regras Anticorrupção.

**CLÁUSULA DÉCIMA QUINTA - PROTEÇÃO DE DADOS**

15.1. A CONTRATANTE declara-se ciente e concorda, bem como adotará todas as medidas para deixar seus parceiros, colaboradores e clientes também cientes, que a CONTRATADA em decorrência do presente Contrato poderá ter acesso, utilizará, manterá e processará, eletrônica e manualmente, informações e dados prestados pela CONTRATANTE e seus clientes (“Dados Protegidos”), exclusivamente para fins específicos do objeto.

15.2. As Partes declaram-se cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) (“LGPD”), e obriga-se a adotar todas as medidas razoáveis para garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD.

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

**CLÁUSULA DÉCIMA SEXTA - DO FORO**

O Foro deste Contrato é a Comarca de Taubaté, do Estado de São Paulo.

E por assim estarem justas e contratadas, as partes assinam o presente Contrato em 02 (duas) vias de igual teor.

Taubaté, ___ de _____ de 2024.

**UNIVERSIDADE DE TAUBATÉ**
**CONTRATANTE**

**CONTRATADA**

## TERMO DE CIÊNCIA E DE NOTIFICAÇÃO (CONTRATOS) *(REDAÇÃO DADA PELA RESOLUÇÃO Nº 11/2021)*

CONTRATANTE:_____
CONTRATADO:_____
CONTRATO Nº (DE ORIGEM):_____
OBJETO: _____

Pelo presente TERMO, nós, abaixo identificados:

**1. Estamos CIENTES de que:**

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais dos responsáveis pela contratante e e interessados estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no Artigo 2º das Instruções nº01/2020, conforme "Declaração(ões) de Atualização Cadastral" anexa (s);

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

**2. Damo-nos por NOTIFICADOS para:**

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

**LOCAL e DATA:** _____

**AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:**

Nome:_____

Cargo:_____

CPF: _____

**RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA DISPENSA/INEXIGIBILIDADE DE LICITAÇÃO:**

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

**RESPONSÁVEIS QUE ASSINARAM O AJUSTE:**

**Pelo contratante:**

UNITAU

**PRA - Pró-reitoria de Administração**
**Serviço de Licitações e Compras**
Avenida 09 de Julho,246 - Centro - Taubaté - SP - 12020-200
fone: (12) 3625-4226/4228 - fax: (12) 3631-2338 / 3624-4005
compras@unitau.br

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

**Pela contratada:**

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

**ORDENADOR DE DESPESAS DA CONTRATANTE:**

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

**GESTOR(ES) DO CONTRATO:**

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

**DEMAIS RESPONSÁVEIS (*):**

Tipo de ato sob sua responsabilidade: _____

Nome:_____

Cargo:_____

CPF: _____

Assinatura: _____

(*) - O Termo de Ciência e Notificação e/ou Cadastro do(s) Responsável(is) deve identificar as pessoas

físicas que tenham concorrido para a prática do ato jurídico, na condição de ordenador da despesa; de partes contratantes; de responsáveis por ações de acompanhamento, monitoramento e avaliação; de responsáveis por processos licitatórios; de responsáveis por prestações de contas; de responsáveis com atribuições previstas em atos legais ou administrativos e de interessados relacionados a processos de competência deste Tribunal. Na hipótese de prestações de contas, caso o signatário do parecer conclusivo seja distinto daqueles já arrolados como subscritores do Termo de Ciência e Notificação, será ele objeto de notificação específica. *(inciso acrescido pela Resolução nº 11/2021)*