



## PROCESSO PRA- 40/18

### PREGÃO PRESENCIAL Nº 19/2018

#### PREÂMBULO

A Universidade de Taubaté – UNITAU, por intermédio do Pregoeiro especialmente designado pelo Magnífico Reitor, torna público que realizará o PREGÃO PRESENCIAL nº 19/2018, do **Tipo Menor Preço**, regido pela Lei federal nº 10.520/02, Lei Complementar 123/06, com alterações da lei complementar nº 147/2014 e pelo Decreto Municipal de Taubaté nº 13.409/14 e subsidiariamente e no que couber pela Lei nº 8.666/93.

#### 1 - DO OBJETO E INÍCIO DA LICITAÇÃO

1.1. A presente licitação tem por objeto a Aquisição de solução de segurança corporativa para endpoints, servidores e rede, consoante com o Anexo I (descrição) e Formulário Padrão (Anexo II) e Minuta de Contrato (Anexo III) que integram o presente Edital.

1.1.1. Critério de julgamento: **Menor Preço Total do Lote.**

1.2. A abertura do presente Pregão será realizada pelo Pregoeiro, em sessão pública, conforme a seguir indicado:

1.2.1. LOCAL: Pró-reitoria de Administração, localizado na Av. Nove de Julho, nº. 246, Centro, cidade de Taubaté, SP, CEP 12020-200, na Sala de Pregão. Informações na Comissão Permanente de Licitações, telefones (12) 3632-8362/3632-7559 e fac-símile (12) 3631-2338.

1.2.2. DATA: 05/06/2018

1.2.3. HORÁRIO: 9h30 (início do credenciamento).

#### 2 – DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1. No dia, hora e local designados para a sessão, os representantes deverão apresentar-se e identificar-se para credenciamento junto ao Pregoeiro.



2.1.1 As empresas que desejarem fazer uso dos benefícios da Lei Complementar 123/06 e suas alterações deverão, no ato do credenciamento, apresentar declaração em papel timbrado e assinado por seu representante legal manifestando o interesse.

2.1.2 Após o credenciamento, será declarada aberta a sessão pela Pregoeira, a partir do que não serão admitidos novos proponentes. Os representantes deverão apresentar declaração de pleno atendimento às exigências do Edital e seus anexos, nos termos do disposto no artigo 4º, VII da Lei 10.520, e entregar os envelopes contendo a Proposta Comercial e os documentos de habilitação.

2.2. As propostas e os documentos de habilitação deverão estar em dois envelopes opacos, lacrados e rubricados no fecho, contendo em suas partes externas e frontais os seguintes dizeres:

**Envelope nº 01**  
**PROPOSTA COMERCIAL**  
**Pregão Presencial nº 19/18**  
**Razão social da empresa**  
**CNPJ**

**Envelope nº 02**  
**DOCUMENTAÇÃO DE HABILITAÇÃO**  
**Pregão Presencial nº 19/18**  
**Razão social da empresa**  
**CNPJ**

2.3. Somente poderão participar deste Pregão pessoas jurídicas constituídas, cujo objeto social seja pertinente e compatível com o objeto deste Pregão, o que deverá ser demonstrado nos termos do subitem 5.1.2, sendo vedada a participação de:

2.3.1. Consórcio de empresas, qualquer que seja sua forma de constituição.

2.3.2. Empresas declaradas inidôneas para licitar ou contratar com a Administração Pública ou punidas, nos termos do art. 87, inciso IV, da Lei Federal nº 8.666/93 e do art. 7º da Lei Federal nº 10.520/2002.

2.3.3. Empresas punidas com suspensão temporária para licitar ou contratar com a Universidade de Taubaté, nos termos do art. 87, inciso III, da Lei Federal nº 8.666/93.

2.4. Os documentos apresentados nesta licitação deverão:

2.4.1. Estar em nome da licitante com o nº do CNPJ e o endereço respectivo, conforme segue:



2.4.1.1. Se a licitante for à matriz, todos os documentos deverão estar em nome da matriz.

2.4.1.2. Se a licitante for à filial, todos os documentos deverão estar em nome da filial.

2.4.2. Estar vigentes na data da abertura, com o prazo de validade estabelecido pelo órgão expedidor em seu corpo;

2.4.3. Ser apresentados em documentos originais ou extraídos diretamente da Internet (original), caso admitido em Lei, ou por qualquer processo de cópia autenticada, ou por cópias não autenticadas, desde que sejam exibidos os originais para conferência e autenticação do Pregoeiro.

### **3 - DO CREDENCIAMENTO**

3.1. O credenciamento far-se-á perante o Pregoeiro, mediante instrumento público ou particular de procuração com firma reconhecida, com poderes para formular ofertas e lances de preços e praticar todos os demais atos pertinentes ao certame, em nome do proponente, bem como com a apresentação de carteira de identidade ou de outro documento equivalente de seu representante legal.

3.1.1. A procuração referida no subitem 3.1 deverá estar acompanhada do estatuto ou contrato social com sua última alteração, devidamente registrado na Junta Comercial ou no órgão competente.

3.1.2. No caso de comparecimento de proprietário, sócio-gerente ou dirigente da empresa, este deverá apresentar o respectivo estatuto ou contrato social, com suas alterações, ou consolidado, devidamente registrados na Junta Comercial ou no órgão competente, no qual estejam expressos poderes para exercer direitos e assumir obrigações em decorrência de tal investidura.

**3.2. Declaração de pleno atendimento às exigências do Edital e seus anexos que deverá ser apresentado no ato do credenciamento.**

3.3. O representante legal do licitante que não se credenciar perante o Pregoeiro ficará impedido de participar da fase de lances verbais, de negociação de preços, de declarar a intenção de interpor recursos, enfim,

de representar a licitante durante a reunião de abertura dos envelopes nº 1 e nº 2, relativos a este Pregão.

3.3.1. Nesta hipótese, o licitante ficará excluído da etapa de lances verbais e mantido o seu preço apresentado na “Proposta Comercial”, para efeito de ordenação das propostas e apuração do menor preço.

## **4 – DA PROPOSTA COMERCIAL**

4.1. A “**PROPOSTA COMERCIAL**” **deverá observar o modelo do Anexo II deste Edital** e ser redigida em língua portuguesa, datilografada ou impressa por meio eletrônico, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, em 01 (uma) via, devidamente datada e assinada, como também rubricadas todas as suas folhas pelo representante da proponente, e ter, **preferencialmente**, seu respectivo número seguido do número total de páginas (exemplo: num total de 37 páginas, a numeração deverá ser a seguinte: 01/37, 02/37 e assim sucessivamente, até 37/37) e dela **deverão constar**:

4.1.1. identificação social, n.º do CNPJ, referência a este Pregão, indicação de endereço eletrônico (e-mail) e fac-símile, se houver, número de telefone, endereço da empresa e dados bancários;

4.1.2. especificação clara, detalhada e suficiente à correta identificação dos produtos cotados, indicando marca e quantidade em conformidade com as especificações contidas no Anexo I e Formulário Padrão de Proposta;

4.1.3. cotação única de preço, observado(s) o(s) respectivo(s) quantitativo(s), apresentando valores em moeda corrente. O preço total deverá ser expresso por extenso;

4.1.3.1. **O critério de julgamento será por preço total do lote**, portanto será desclassificada a proposta que não atender a todas as especificações constantes nos Anexos I (descrição) e II (Formulário de Proposta Comercial).

4.1.4. prazo de instalação será conforme Anexo I – Termo de Referência e Minuta de Contrato (Anexo III).

4.1.5. pagamento: será conforme Anexo I – Termo de Referência e Minuta de Contrato (Anexo III).



4.1.6. prazo mínimo de validade da proposta: 60 (sessenta) dias, contados da data da sessão de recebimento dos envelopes nº 1 e nº 2;

**4.1.7. A licitante poderá substituir as condições expressas no subitem 4.1.4. até 4.1.6, presentes na Proposta Comercial, pela expressão “de acordo com o Edital”, pois o preenchimento diverso ao previsto no Edital desclassificará a empresa.**

4.2. O valor total ofertado será irrevogável e deverá corresponder ao preço final, nele incluídos os acréscimos constantes do item V da Proposta Comercial (Anexo II) ou benefícios que afetem o valor dos serviços e materiais, tais como isenções, imunidades ou outros de qualquer natureza, de sorte que o preço indicado na Proposta Comercial do licitante corresponda ao valor final a ser despendido pela UNITAU.

4.3. Após a abertura da sessão (item 2.2. deste Edital), não serão admitidos pedidos de desistência, retificação de preços ou de quaisquer outras condições oferecidas.

**4.4. A proposta apresentada em desacordo com o disposto neste edital será desclassificada.**

4.5. O intervalo mínimo de valor para cada lance será de R\$ 500,00 (quinhentos reais) para o LOTE.

4.6. A negociação levará em conta o valor total da proposta apresentada, cabendo ao licitante vencedor informar posteriormente os preços unitários para cada item.

## **5 - DA DOCUMENTAÇÃO PARA HABILITAÇÃO**

5.1. Os documentos para habilitação, a serem apresentados na forma do subitem 2.4 e que deverão constar do envelope “DOCUMENTAÇÃO”, serão os seguintes:

5.1.1. Registro Comercial, no caso de empresa individual.

5.1.2. Ato Constitutivo, Estatuto ou Contrato Social em vigor, cópia autenticada ou cópia simples acompanhada do original para autenticação, 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.

5.1.2.1. No caso da apresentação da documentação referente ao subitem 5.1.2 na fase de credenciamento, poderá a licitante deixar de apresentá-lo no envelope de documentos.

5.1.3. 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.

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

5.1.5. 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).

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

5.1.7. Certidão Negativa relativa à Imposto de Circulação de Mercadorias e Serviços (ICMS), expedida pelo órgão fazendário estadual, ou declaração de isenção ou de não incidência, assinada pelo (s) representante (s) legal (is) da empresa, sob as penas da lei.

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

5.1.9. Declaração de cumprimento do disposto no art. 7º, XXXIII, da Constituição Federal/88, conforme inciso V do artigo 27 da Lei Federal nº 8.666/93, em papel timbrado do licitante de que não mantém em seu quadro de empregados menores de 16 anos, nem menores de 18 anos em trabalho noturno, perigoso ou insalubre.

5.1.10. 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.

5.1.11. Certidão Negativa de Licitantes Inidôneos, disponível no site do Tribunal de Contas da União e Relação de Impedimentos de Contratos/Licitação emitida no Tribunal de Contas do Estado de São Paulo.

5.1.12. Caso a licitante declarada vencedora seja uma Microempresa e Empresa de Pequeno Porte, a mesma terá 05 (cinco) dias úteis, prorrogados por igual período a critério da Administração Pública, para regularizar pendências **FISCAIS**, caso esta apresente alguma restrição, conforme o disposto nos artigos 42 e 43 da Lei Complementar 123/2006 e suas alterações, ressaltando que **RESTRIÇÃO** não há que se confundir com certidão com prazo de validade vencido, situação válida somente para as **certidões de natureza fiscal**.

5.1.13. Caso a Microempresa ou Empresa de Pequeno Porte que se beneficiar no disposto no subitem 5.1.12 não o fizer dentro do prazo estipulado no mesmo subitem, será convocada a segunda licitante melhor classificada para a verificação de suas condições habilitatórias, e assim sucessivamente até que aconteça a habilitação de uma das licitantes.

## **6 – DA ABERTURA E JULGAMENTO DAS PROPOSTAS**

6.1. Abertos os envelopes, as propostas serão rubricadas pelo Pregoeiro.

6.2. Examinadas as propostas e verificada sua conformidade com as especificações estabelecidas no Formulário Padrão de Proposta (Anexo II) e lidos os preços, o Pregoeiro relacionará todas as propostas em ordem crescente de valor. Em seguida, classificará o autor da proposta de menor preço e aqueles que tenham apresentado propostas em valores sucessivos e superiores em até 10 % (dez por cento), relativamente à proposta de menor preço global, em se tratando de item único, ou menor preço por item, havendo mais de um item, objeto da licitação.

6.3. Se a proposta contiver algum ponto que dificulte ou impossibilite sua clara compreensão, o pregoeiro poderá solicitar esclarecimento ao representante da licitante, sendo vedada a inclusão de documento novo.

6.3.1. Constatado que está(ão) ausente(s) informação(ões) fundamental(is) na proposta, a licitante será desclassificada do certame.

6.4. Quando não forem verificadas, no mínimo, 03 (três) propostas escritas de preços nas condições definidas no subitem 6.2., o Pregoeiro



classificará as melhores propostas subseqüentes, até o máximo de 3 (três), para que suas autoras participem dos lances verbais, quaisquer que sejam os preços oferecidos nas Propostas Comerciais.

6.5. Em seguida, será dado início à etapa de apresentação de lances verbais de forma seqüencial, a partir da autora da proposta de maior preço e os demais em ordem decrescente de valor, sendo que, no caso de empate de preço, a precedência do lance será decidida por sorteio.

6.6. Os lances verbais devem ser inferiores ao da proposta de menor preço.

6.6.1. Caso o objeto do Pregão tenha mais de um Lote, o Pregoeiro realizará a etapa de lances para todos os Lotes, para só então iniciar a etapa de habilitação dos licitantes que tiverem oferecido o menor preço.

6.7. A desistência ao direito de apresentar lance verbal implicará a exclusão da licitante dessa etapa, sendo considerado o preço de sua Proposta Comercial para efeito de classificação das ofertas.

6.8. Não havendo mais interessados em apresentar lance verbal, será encerrada a etapa competitiva e serão ordenadas as propostas pelo critério de menor preço global, em se tratando de Lote único, ou menor preço por item, havendo mais de um item.

6.9. Caso não se realize lances verbais, ou a empresa classificada em primeiro lugar seja inabilitada, o Pregoeiro poderá, a seu critério, negociar diretamente com a proponente da melhor proposta para que seja obtido preço melhor.

6.10. O Pregoeiro examinará a aceitabilidade da primeira proposta classificada, quanto ao objeto e valor, suspendendo a sessão para a análise dos documentos referidos no item 5 e seus subitens, e, em seguida, decidirá motivadamente, conforme definido neste Edital e seus anexos.

6.11. Será classificado em 1º lugar a licitante que apresentar a proposta de menor preço global, em se tratando de Lote único, ou menor preço por item, havendo mais de um item, cujo objeto lhe(s) será(ão) adjudicado(s), caso seja(m) habilitado(s).

6.12. Quando o critério de julgamento for o de menor preço global, em se tratando de Lote único composto de mais de um bem, a licitante





vencedora deverá, após 02 dias da adjudicação, fornecer o valor unitário de cada bem.

6.12.1. Após a reunião do Pregão, o licitante vencedor terá **dois dias úteis** para apresentar (por e-mail, fac-símile etc.) nova planilha com os novos preços diluídos. Os novos preços diluídos deverão respeitar os valores de mercado. O vencedor não poderá supervalorizar o valor de um item em detrimento de outro. Cabe lembrar que a Lei 8666/93 em seu Art. 48, II, condena a apresentação de preços manifestadamente inexequíveis.

## 7 - DA HABILITAÇÃO

### 7.1. Habilitação jurídica

7.1.1 Será aberto o envelope contendo a documentação do licitante classificado em 1º lugar, para confirmação de suas condições habilitatórias, cabendo ao pregoeiro obter esclarecimentos relativos à documentação na própria sessão, vedada a inclusão de documento novo.

7.1.2. Se, apesar do saneamento previsto no subitem anterior, a licitante classificada não atender às exigências para a habilitação, o Pregoeiro examinará a oferta subsequente de menor preço, verificando sua aceitabilidade quanto ao objeto e valor, conforme previsto no subitem 6.10, bem como verificará as condições de habilitação de sua autora, e assim sucessivamente, até a apuração de uma oferta aceitável, cuja autora atenda aos requisitos de habilitação, caso em que será declarada vencedora e a ela adjudicado o objeto do certame.

7.1.3. Na hipótese do subitem 7.1.2., o Pregoeiro poderá negociar diretamente com a licitante para que seja obtido o melhor preço.

7.1.4. Os documentos de habilitação (envelope nº. 2) de todos os participantes deste Pregão ficarão mantidos na UNITAU até a finalização da entrega do objeto, após o que os licitantes terão o prazo de 3 (três) dias para solicitar a sua devolução, sendo inutilizados decorridos tal prazo.

7.1.5. Caso a licitante declarada vencedora seja uma Microempresa e Empresa de Pequeno Porte, a mesma terá 05 (cinco) dias úteis, prorrogados por igual período a critério da Administração Pública, para regularizar pendências **FISCAIS**, caso esta apresente alguma restrição, conforme o disposto nos artigos 42 e 43 da Lei Complementar 123/2006 e suas alterações, ressaltando que **RESTRIÇÃO** não há que se confundir com

certidão com prazo de validade vencido, situação válida somente para as **certidões de natureza fiscal**.

7.1.6. Caso a Microempresa ou Empresa de Pequeno Porte que se beneficiar no disposto no subitem 7.5 não o fizer dentro do prazo estipulado no mesmo subitem, será convocada a segunda licitante melhor classificada para a verificação de suas condições habilitatórias, e assim sucessivamente até que aconteça a habilitação de uma das licitantes.

## **7.2 Qualificação Técnica**

7.2.1. O atestados de Qualificação Técnica deverão ser apresentados conforme Termo de Referência (Anexo I).

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

7.2.5. O(s) documento(s) devem 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).

7.2.6. 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 EMPRESA; outros dados característicos; e a identificação da pessoa jurídica emitente bem como o nome e o cargo do signatário.

## **8- DA IMPUGNAÇÃO, DOS RECURSOS, DA HOMOLOGAÇÃO E DA ADJUDICAÇÃO**

8.1. Até 02 (dois) dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa, física ou jurídica, poderá impugnar este Edital de Pregão.

8.2. Caberá ao Pregoeiro decidir sobre a impugnação no prazo máximo de 24 (vinte e quatro) horas antes da data marcada para a Sessão.

8.3. Acolhida a impugnação contra o Edital, será designada nova data para a realização do certame, dando conhecimento aos interessados.



8.4. Declarada à vencedora, qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, com registro em ata da síntese de suas razões, quando lhe será concedido o prazo de 03 (três) dias para apresentação das razões do recurso, ficando as demais licitantes intimados para apresentar contra-razões em igual prazo, que começará a correr do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos autos.

8.5. A falta de manifestação imediata e motivada da licitante ou da apresentação das razões do recurso, de que dispõe o subitem anterior, importará na preclusão dessa fase processual e a adjudicação do(s) objeto(s) da licitação à vencedora, pelo Pregoeiro, seguindo-se a homologação pela autoridade competente.

8.6. Os recursos interpostos em face das decisões do Pregoeiro terão efeito suspensivo.

8.7. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

8.8. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade competente fará a adjudicação do(s) objeto(s) da licitação à(s) licitante(s) vencedora(s) e homologará o procedimento.

## **9 - DAS COMINAÇÕES**

9.1. Ficará impedido de licitar e contratar com a Administração, pelo prazo de até 02 (dois) anos, ou enquanto perdurarem os motivos determinantes da punição, o licitante que, convocado dentro do prazo de validade de sua proposta, não assinar o contrato ou instrumento equivalente, não entregar documentação exigida para o certame, apresentar documentação falsa, ensejar o retardamento da execução do objeto da contratação, não mantiver a proposta, lance ou oferta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, sendo-lhe assegurada a defesa prévia.

9.2. As demais serão aplicadas conforme descrito na Minuta de Contrato (Anexo III).



**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

## **10 – DA CONTRATAÇÃO**

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

10.2. A adjudicatária deverá assinar o contrato relativo ao objeto adjudicado, no prazo de 05 (cinco) dias úteis, a contar da data da Notificação do Setor de Contratos.

10.2.1. A recusa injustificada da licitante vencedora em assinar o Contrato, caracterizará o descumprimento total da obrigação assumida, considerando-se decaído seu direito de vencedor e sujeitando-o às penalidades previstas no item 09 e seus subitens.

10.2.2. É facultado à UNITAU, na hipótese de recusa da licitante vencedora em assinar o contrato, convocar para contratação, em sessão pública, as licitantes remanescentes, respeitada a ordem de classificação.

10.2.3. Não serão apenadas as licitantes convocadas na forma do subitem 10.2.2. supra que não concordarem em celebrar o contrato.

10.3. O prazo de vigência deste instrumento será conforme a Minuta de Contrato (Anexo III).

## **11 – DO PRAZO DE ENTREGA E DO RECEBIMENTO**

11.1. O objeto será recebido pela Central de TI da UNITAU, telefone (12) 3632-3195 e (12) 3635-5244, email [infra@unitau.br](mailto:infra@unitau.br), sendo responsável o Coordenador da Central de Tecnologia da Informação Sr<sup>a</sup> Edilene Dutra de Moraes Fonseca, que indicará o local de instalação. A entrega e instalação deverão ser agendadas nos telefones informados.

11.2. Os prazos e condições de entrega serão conforme descrito no Anexo I – Termo de Referência e Minuta de Contrato (Anexo III).

## **12 - DO PAGAMENTO**

12.1. O pagamento será efetuado conforme Anexo I – Termo de Referência e Minuta de Contrato (Anexo III).

## **13 – DA CAUÇÃO**

13.1. No ato da assinatura do contrato o licitante vencedor deverá apresentar caução equivalente a 5% (cinco por cento) do valor inicial, por qualquer das modalidades abaixo:

- a) depósito em dinheiro ou títulos da dívida pública;
- b) seguro garantia;
- c) fiança bancária.

**13.2.** A expressão monetária da caução deverá ser mantida sempre que se alterar o valor contratual, preservando-se, assim, o percentual de 5% (cinco por cento), mas seu valor será liberado integralmente apenas ao final da execução contratual satisfatória; ou pelo saldo, se houver, procedidos eventuais descontos.

## **14 – DAS DISPOSIÇÕES FINAIS**

14.1. O Edital estará disponível na sala da Comissão Permanente de Licitação, localizada na Avenida Nove de Julho, nº 246, Centro – Taubaté – SP, no valor de R\$ 10,00, informações pelos telefones (12) 3632-8362/3632-7559. O Edital também estará disponível (gratuitamente), para download, na página da UNITAU na Internet, no endereço [www.unitau.br](http://www.unitau.br).

14.2. Nenhuma indenização será devida às empresas licitantes pela elaboração de proposta ou apresentação de documentos relativos a esta licitação.

14.3. Quando todos os licitantes forem desclassificados ou inabilitados, poderá o Pregoeiro fixar-lhes o prazo de 02 (dois) dias para apresentação de outras propostas ou novas documentações escoimadas das causas que ensejaram o ato de desclassificação ou inabilitação.

14.4. Da sessão será lavrada ata com a relação das empresas licitantes e todas as ocorrências que interessarem ao certame, conforme previsto no Regulamento do Pregão. Essa ata será assinada pelo pregoeiro e pelos licitantes presentes na sessão.



14.5. Sem prejuízo das disposições contidas no Capítulo III da Lei Federal nº 8.666/93, o presente Edital e a proposta da adjudicatária serão partes do Termo de Contrato ou instrumento equivalente.

14.6. O Termo de Contrato ou instrumento equivalente poderá ser alterado nos casos previstos no art. 65 da Lei Federal nº 8.666/93, desde que haja interesse da Administração.

14.7. O Pregoeiro, ou autoridade superior, poderá promover diligências destinadas a elucidar ou complementar a instrução do processo, em qualquer fase da licitação, fixando prazos para atendimento.

14.8. O Pregoeiro ou autoridade superior poderá subsidiar-se em pareceres emitidos por técnicos ou especialistas na matéria objeto desta licitação.

14.9. Consultas **deverão** ser dirigidas ao Pregoeiro por meio do e-mail **questionamentos@unitau.br**. Não utilizar outro email para formular perguntas, pois não são de acesso do Pregoeiro e da Equipe de Apoio. Ou pessoalmente no Serviço de Licitações da UNITAU.

14.10. Toda comunicação oficial dar-se-á pelo “site” [www.unitau.br](http://www.unitau.br) e por publicação, nos termos da legislação vigente.

14.10.1. As dúvidas decorrentes da interpretação deste Edital e as informações adicionais, que se fizerem necessárias à elaboração das Propostas, deverão ser apresentadas por escrito ou e-mail, conforme informações constantes do item 01 deste Edital, até o prazo de 02 (dois) dias úteis antes da abertura da licitação. Entende-se neste caso como dia útil aqueles em que houver expediente na UNITAU.

14.10.2. O Pregoeiro responderá os questionamentos em até 01 (um) dia útil antes da data prevista para abertura da licitação por meio do site da Universidade ([www.unitau.br](http://www.unitau.br)). Entende-se neste caso como dia útil aqueles em que houver expediente na UNITAU.

14.10.3. Os pedidos de esclarecimentos de que trata o subitem 14.10.1, não constituirão, necessariamente, motivos para que se altere a data e o horário do Pregão.

14.10.4. Para as respostas às consultas formuladas, o Pregoeiro utilizar-se de meios eletrônicos divulgando a resposta por meio do site da Universidade ([www.unitau.br](http://www.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

14.11. O resultado final deste procedimento licitatório será divulgado por meio de publicação no Diário Oficial do Estado de São Paulo, com indicação da modalidade, do número de ordem e da série anual, do objeto, do valor total e da licitante vencedora.

*Taubaté, 16 de maio de 2018.*

***Márcia Regina Rosa  
Pregoeira***



## **ANEXO I**

### **PREGÃO PRESENCIAL Nº 19/2018**

| <b>LOTE</b> | <b>DESCRIÇÃO</b>  | <b>UNIDADE</b>  | <b>QUANTIDADE</b> |
|-------------|---|-----------------|-------------------|
| <b>01</b>   | Solução de segurança corporativa para endpoints, servidores e rede. | <b>Licenças</b> | <b>1.500</b>      |

#### **Central de Tecnologia da Informação**

#### **TERMO DE REFERÊNCIA**

### **SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, SERVIDORES E REDE UNITAU**

#### **I Objeto**

**NOME:** AQUISIÇÃO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, SERVIDORES E REDE UNITAU.

#### **II Motivação**

Na tecnologia de informação e comunicação (TIC) as ameaças à segurança tem crescido de forma galopante nos últimos anos. Hoje são necessárias várias camadas de proteção tanto na rede, servidores, emails, 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 este ano e ano passado 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 outras já existentes não deve duplicar funções já existentes mas cobrir as áreas ainda não cobertas pelas outras camadas de soluções.

#### **III Especificações técnicas**

##### **1. Servidor de Administração e Console Administrativa**

###### **1.1. Compatibilidade no mínimo com:**

- Microsoft Windows 10 Pro 32-bit / 64-bit.
- Microsoft Windows 10 RS2 32-bit / 64-bit.
- Microsoft Windows 10 Enterprise 32-bit / 64-bit.
- Microsoft Windows 10 Education 32-bit / 64-bit.
- Microsoft Windows 10 Pro RS1 32-bit / 64-bit.
- Microsoft Windows 10 Enterprise RS1 32-bit / 64-bit.
- Microsoft Windows 10 Education RS1 32-bit / 64-bit.
- Microsoft Windows 8.1 Pro 32-bit / 64-bit.
- Microsoft Windows 8.1 Enterprise 32-bit / 64-bit.
- Microsoft Windows 8 Pro 32-bit / 64-bit.



- Microsoft Windows 8 Enterprise 32-bit /64-bit.
  - Microsoft Windows 7 Professional SP1 32-bit / 64-bit.
  - Microsoft Windows 7 Enterprise SP1 32-bit / 64-bit.
  - Microsoft Windows 7 Ultimate SP1 32-bit / 64-bit.
  - Microsoft Small Business Server 2008 Standard 64-bit.
  - Microsoft Small Business Server 2008 Premium 64-bit.
  - Microsoft Small Business Server 2011 Essentials 64-bit.
  - Microsoft Small Business Server 2011 Premium Add-on 64-bit.
  - Microsoft Small Business Server 2011 Standard 64-bit.
  - Microsoft Windows Server 2008 Datacenter SP1 32-bit / 64-bit.
  - Microsoft Windows Server 2008 Enterprise SP1 32-bit / 64-bit.
  - Microsoft Windows Server 2008 Foundation SP2 32-bit / 64-bit.
  - Microsoft Windows Server 2008 SP1 32-bit / 64-bit.
  - Microsoft Windows Server 2008 Standard SP1 32-bit / 64-bit.
  - Microsoft Windows Server 2008.
  - Microsoft Windows Server 2008 R2 Server Core 64-bit.
  - Microsoft Windows Server 2008 R2 Datacenter 64-bit.
  - Microsoft Windows Server 2008 R2 Datacenter SP1 64-bit.
  - Microsoft Windows Server 2008 R2 Enterprise 64-bit.
  - Microsoft Windows Server 2008 R2 Enterprise SP1 64-bit.
  - Microsoft Windows Server 2008 R2 Foundation 64-bit.
  - Microsoft Windows Server 2008 R2 Foundation SP1 64-bit.
  - Microsoft Windows Server 2008 R2 SP1 Core Mode 64-bit.
  - Microsoft Windows Server 2008 R2 Standard 64-bit.
  - Microsoft Windows Server 2008 R2 Standard SP1 64-bit.
  - Microsoft Windows Server 2012 Server Core 64-bit.
  - Microsoft Windows Server 2012 Datacenter 64-bit.
  - Microsoft Windows Server 2012 Essentials 64-bit.
  - Microsoft Windows Server 2012 Foundation 64-bit.
  - Microsoft Windows Server 2012 Standard 64-bit.
  - Microsoft Windows Server 2012 R2 Server Core 64-bit.
  - Microsoft Windows Server 2012 R2 Datacenter 64-bit.
  - Microsoft Windows Server 2012 R2 Essentials 64-bit.
  - Microsoft Windows Server 2012 R2 Foundation 64-bit.
  - Microsoft Windows Server 2012 R2 Standard 64-bit.
  - Windows Storage Server 2008 R2 64-bit.
  - Windows Storage Server 2012 64-bit.
  - Windows Storage Server 2012 R2 64-bit.
  - Microsoft Windows Server 2016 64-bit.
- 1.2. Possuir Compatibilidade, no mínimo, as seguintes plataformas virtuais:**
- Vmware: esxi 5.5, esxi 6.0;
  - Vmware VSphere 5.5
  - Vmware VSphere 6
  - Microsoft Hyper-V: 2012, 2012 r2;

### **1.3. Possuir Compatibilidade, no mínimo, os seguintes Gerenciadores de Bancos de Dados:**

- Microsoft SQL Server 2008 Express 32-bit.
- Microsoft SQL 2008 R2 Express 64-bit.
- Microsoft SQL 2012 Express 64-bit.
- Microsoft SQL 2014 Express 64-bit.
- Microsoft SQL Server 2008 32-bit / 64-bit.
- Microsoft SQL Server 2008 R2 64-bit.
- Microsoft SQL Server 2008 R2 Service Pack 2 64-bit.
- Microsoft SQL Server 2012 64-bit.
- Microsoft SQL Server 2014 64-bit.
- Microsoft SQL Server 2016 64-bit.

### **1.4. Console Administrativa Web integrada com o Servidor de Administração**

#### **1.4.1. Compatibilidade, no mínimo, com os seguintes Sistemas Operacionais:**

- Microsoft Windows 10 Pro 32-bit / 64-bit.
- Microsoft Windows 10 RS2 32-bit / 64-bit.
- Microsoft Windows 10 Enterprise 32-bit / 64-bit.
- Microsoft Windows 10 Education 32-bit / 64-bit.
- Microsoft Windows 10 Pro RS1 32-bit / 64-bit.
- Microsoft Windows 10 Enterprise RS1 32-bit / 64-bit.
- Microsoft Windows 10 Education RS1 32-bit / 64-bit.
- Microsoft Windows 8.1 Pro 32-bit / 64-bit.
- Microsoft Windows 8.1 Enterprise 32-bit / 64-bit.
- Microsoft Windows 8 Pro 32-bit / 64-bit.
- Microsoft Windows 8 Enterprise 32-bit / 64-bit.
- Microsoft Windows 7 Professional SP1 32-bit / 64-bit.
- Microsoft Windows 7 Enterprise SP1 32-bit / 64-bit.
- Microsoft Windows 7 Ultimate SP1 32-bit / 64-bit.
- Microsoft Small Business Server 2008 Standard 64-bit.
- Microsoft Small Business Server 2008 Premium 64-bit.
- Microsoft Small Business Server 2011 Essentials 64-bit.
- Microsoft Small Business Server 2011 Premium Add-on 64-bit.
- Microsoft Small Business Server 2011 Standard 64-bit.
- Microsoft Windows Server 2008 Datacenter SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Enterprise SP1 32-bit / 64-bit.
- Microsoft Windows Server 2008 Foundation SP2 32-bit / 64-bit.
- Microsoft Windows Server 2008.
- Microsoft Windows Server 2008 R2 Server Core 64-bit.
- Microsoft Windows Server 2008 R2 Datacenter 64-bit.
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-bit.
- Microsoft Windows Server 2008 R2 Enterprise 64-bit.
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-bit.
- Microsoft Windows Server 2008 R2 Foundation 64-bit.
- Microsoft Windows Server 2008 R2 Foundation SP1 64-bit.
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-bit.

- Microsoft Windows Server 2008 R2 Standard 64-bit.
- Microsoft Windows Server 2008 R2 Standard SP1 64-bit.
- Microsoft Windows Server 2012 Server Core 64-bit.
- Microsoft Windows Server 2012 Datacenter 64-bit.
- Microsoft Windows Server 2012 Essentials 64-bit.
- Microsoft Windows Server 2012 Foundation 64-bit.
- Microsoft Windows Server 2012 Standard 64-bit.
- Microsoft Windows Server 2012 R2 Server Core 64-bit.
- Microsoft Windows Server 2012 R2 Datacenter 64-bit.
- Microsoft Windows Server 2012 R2 Essentials 64-bit.
- Microsoft Windows Server 2012 R2 Foundation 64-bit.
- Microsoft Windows Server 2012 R2 Standard 64-bit.
- Windows Storage Server 2008 R2 64-bit.
- Windows Storage Server 2012 64-bit.
- Windows Storage Server 2012 R2 64-bit.
- Microsoft Windows Server 2016 64-bit.
- Debian GNU/Linux 8.x 32-bit.
- Debian GNU/Linux 8.x 64-bit.
- Ubuntu Server 16.04 LTS 32-bit.
- Ubuntu Server 16.04 LTS 64-bit.
- Ubuntu Server 14.04 LTS 32-bit.
- Ubuntu Server 14.04 LTS 64-bit.
- CentOS 7.0 64-bit.
- CentOS 6.x (up to 6.6) 64-bit.
- Red Hat Enterprise Linux Server 7.x 64-bit.
- SUSE Linux Enterprise Server 12 64-bit.

**1.5. Possuir compatibilidade, no mínimo, com os seguintes navegadores:**

- Microsoft® Edge.
- Chrome™ 53 e mais recente.
- Firefox™ 47 e mais recente.
- Safari 8 em Mac OS x 10.10 (Yosemite).
- Safari 9 no Mac OS x 10.11 (El Capitan).

**1.6. Características mínimas obrigatórias e nativas da solução em uma console única de gerenciamento:**

- 1.6.1. A console deve ser acessada via web (https);
- 1.6.2. O gerenciamento de ser em português;
- 1.6.3. Console deve ser baseada no modelo cliente/servidor;
- 1.6.4. Possuir capacidade de importar uma licença adicional do produto
- 1.6.5. Possuir capacidade de fornecer estatísticas de status da proteção, níveis de vulnerabilidades, instalação, atualização, vírus, correções de vulnerabilidades
- 1.6.6. Possuir capacidade de gerar relatórios gráficos, de no mínimo:
  - Relatório do status de proteção
  - Relatório de Erros
  - Relatório de Eventos
  - Relatório dos repositórios remotos de instalação e atualização
  - Relatório dos servidores secundários de balanceamento

- Relatório de uso da chave
  - Relatórios de versões da proteção Endpoint
  - Relatório de Instalação da Proteção Endpoint
  - Relatório de atualização de vacinas e versão da proteção do Endpoint
  - Relatório de vírus
  - Relatório de computadores mais infectados
  - Relatório de ataque de rede
  - Relatório de aplicativos instalados
  - Relatório de usuários de computadores mais infectados
  - Relatório vulnerabilidades
- 1.6.7. Permitir o envio de relatórios por email, com possibilidade de definir data e horário em que o relatório será enviado.
- 1.6.8. Permitir salvar os relatórios em um diretório local e diretório de rede, com possibilidade de definir data e horário em que o relatório será salvo.
- 1.6.9. Dashboard nativo na Console de Gerenciamento, com os principais relatórios (detecção, instalação, rastreamento, atualização).
- 1.6.10. Possuir log centralizado de todos os eventos envolvendo a proteção e console de gerenciamento.
- 1.6.11. Permitir o registro de eventos no SO em que o Servidor de Administração do Endpoint está instalado.
- 1.6.12. Permitir o envio das notificações dos eventos no mínimo, por email, SNMP.
- 1.6.13. Permitir a execução de scripts externos, em caso de notificações que necessitam de uma resposta rápida e automática.
- 1.6.14. Permitir a alteração das portas padrões de comunicação do Servidor de Administração, Console Administrativa e clientes.
- 1.6.15. Permitir que o Servidor de Administração habilite uma política restritiva em casos de epidemias.
- 1.6.16. Possuir capacidade de definir direitos e funções para os usuários do Servidor de Administração, exemplo (funções básicas, análise de eventos, instalação da proteção, relatório de chaves, dentre outros).
- 1.6.17. Possuir capacidade de eleger repositórios na rede, para distribuição das atualizações e instalações.
- 1.6.18. Permitir a configuração de servidor proxy para conexão com a rede WAN.
- 1.6.19. Possuir capacidade de realizar a contagem das ameaças identificadas nos computadores com relatório gráfico em no mínimo PDF.
- 1.6.20. Permitir a pesquisa de computadores na Console de Gerenciamento, por no mínimo os seguintes parâmetros:
- Nome do Computador
  - Intervalo de IP
  - Versão de a proteção instalada
  - Sistema Operacional
  - Maquinas virtuais
  - Vulnerabilidades
  - Número de detecção de vírus
  - Computadores com verificação de vírus pendente
  - Computadores que há muito tempo não se conectam no Servidor de Administração
- 1.6.21. Possuir capacidade de criar estrutura de grupos de computadores de acordo com o planejamento da rede

- 1.6.22. Possuir capacidade de criar a estrutura de grupos baseado no Diretório Ativo.
- 1.6.23. Possuir capacidade de criar a estrutura de grupos baseado no Domínio de Rede.
- 1.6.24. Possuir capacidade de forçar a sincronização entre o Servidor de Administração e o Cliente.
- 1.6.25. Possuir capacidade de enviar uma mensagem customizada ao computador cliente.
- 1.6.26. Possuir capacidade de adicionar um servidor de administração secundário ou escravo.
- 1.6.27. Possuir capacidade de adicionar um servidor de administração virtual.
- 1.6.28. Possuir capacidade de identificar máquinas que não possui a proteção instalada.
- 1.6.29. Possuir capacidade de remanejar automaticamente computadores desprotegidos para grupos de instalação automática da proteção Endpoint
- 1.6.30. Possuir capacidade de parar e iniciar remotamente e separadamente os módulos da proteção Endpoint ou a proteção por completo.
- 1.6.31. Possuir capacidade de obter individualmente as seguintes informações de cada computador com a proteção Endpoint:
- Nome
  - Domínio
  - Nome no domínio
  - Endereço IP
  - Grupo do Servidor de Administração
  - Última Atualização
  - Última hora visível na rede
- 1.6.32. Permitir a conexão direta com o cliente sem intervalos de conexão.
- 1.6.33. Possuir capacidade de exibir e exportar em arquivo, todos os aplicativos instalados em cada computador.
- 1.6.34. Possuir capacidade de exibir e exportar em arquivo, todos os executáveis em cada computador.
- 1.6.35. Possuir capacidade de exibir e exportar em arquivo, as informações de hardware de cada computador.
- 1.6.36. Possuir capacidade de exibir o usuário que está conectado ao computador.
- 1.6.37. Possuir capacidade de listar as vulnerabilidades conhecidas de cada software instalado em no computador.
- 1.6.38. Possuir capacidade de listar o repositório atual em que o computador está baixando as atualizações.
- 1.6.39. Possuir política única com as opções de configuração para todos os módulos da proteção Endpoint.
- 1.6.40. Possuir capacidade de criar política com herança de uma política precursora.
- 1.6.41. Possuir capacidade de criar no mínimo as seguintes tarefas para gestão e configuração do produto:
- Adicionar chave
  - Alterar componentes do aplicativo
  - Atualização do banco de dados
  - Reverter a versão do banco de dados de assinaturas de vírus
  - Verificação de vírus
  - Instalar aplicativos remotamente
  - Instalar atualizações requeridas e corrigir vulnerabilidades

1.6.42. Possuir capacidade de realizar backup das configurações do Servidor de Administração.

1.6.43. Permitir a classificação dos computadores com no mínimo os seguintes parâmetros:

- Novos computadores encontrados
- Computadores com status crítico
- Computadores com status de advertência
- Computadores sem proteção Endpoint
- Computadores que perderam a conexão com o Servidor de Administração
- Computadores com a proteção Endpoint desativada
- Computadores com suspeita de epidemia de vírus
- Computadores em que a verificação de vírus não é executada
- Computadores com banco de dados desatualizados
- Computadores com sistema e aplicações vulneráveis
- Permitir seleção de computadores por tipo e versão de Sistema Operacional
- Permitir seleção de computadores por range de IP ou subnets
- Permitir seleção de computadores por diretório ativo
- Permitir seleção de computadores por tipo virtual ou físico

1.6.44. Possuir capacidade de descobrir os computadores novos na rede e realizar instalação automática da proteção Endpoint.

1.6.45. Possuir capacidade de listar e atribuir funções aos usuários do domínio.

1.6.46. Possuir capacidade de listar todos os aplicativos encontrados nos computadores da rede.

1.6.47. Possuir capacidade de corrigir automaticamente as vulnerabilidades detectadas nos computadores da rede.

1.6.48. Possuir capacidade de realizar instalação remota da proteção Endpoint nos computadores.

1.6.49. Possuir capacidade de importar aplicativos de terceiros para implementação remota nos computadores gerenciados.

1.6.50. Possuir capacidade de desinstalar remotamente a proteção Endpoint.

1.6.51. Possuir capacidade de desinstalar remotamente softwares de terceiros e antivírus de outros fabricantes.

1.6.52. Possuir capacidade de exportar os pacotes de instalações para implementação no modo stand-alone.

1.6.53. Possuir capacidade de realizar instalação através de GPO e script de login.

1.6.54. Permitir o gerenciamento da proteção em Dispositivos Mobiles (Smartphones e Tablets) sem necessidade de instalar uma console adicional.

1.6.55. Possuir capacidade de realizar a descoberta de novos computadores na rede através de no mínimo das seguintes maneiras:

- Diretório Ativo
- Domínio de Rede
- Subnets
- Netbios
- Range de IP

1.6.56. Permitir a possibilidade de restauração de arquivos em área de quarentena.

1.6.57. Possuir compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

1.6.58. Deve permitir a atribuição de perfis para os administradores e operadores da Console de Gerenciamento.

1.6.59. Console única e totalmente integrada com todas as funções e módulos da proteção Endpoint.

1.6.60. As licenças deverão ser perpétuas, ou seja, expirada a validade das mesmas o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

1.6.61. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

1.6.62. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

1.6.63. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

1.6.64. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

1.6.65. Possuir capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

1.6.66. Possuir capacidade de gerenciar smartphones e tablets (Android) protegidos pela solução de segurança;

1.6.67. A comunicação entre o Cliente e o Servidor de Administração deve ser criptografada;

1.6.68. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou Endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema operacional;
- Máquina virtual.

1.6.69. Possuir capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.6.70. Possuir capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para ser adicionada a proteção;

1.6.71. Possuir capacidade de detectar máquinas novas no Active Directory, subnets ou grupos de trabalho e automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.6.72. Possuir capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias;

1.6.73. Possuir capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.6.74. Deve fornecer no mínimo as seguintes informações dos computadores:

- Se o antivírus está instalado;
- Se o antivírus está iniciado;
- Se o antivírus está atualizado;
- Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- Minutos/horas desde a última atualização de vacinas;

- Data e horário da última verificação executada na máquina;
  - Versão do antivírus instalado na máquina;
  - Se é necessário reiniciar o computador para aplicar mudanças;
  - Quantidade de vírus encontrados (contador) na máquina;
  - Nome do computador;
  - Domínio ou grupo de trabalho do computador;
  - Sistema operacional com service pack;
  - Usuário (s) logado(s) naquele momento, com informações de contato (caso disponíveis no active directory);
  - Endereço IP;
  - Vulnerabilidades de aplicativos instalados na máquina;
- 1.6.75. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 1.6.76. Possuir capacidade de reconectar máquinas clientes ao servidor de administração mais próximo, baseado em regras de conexão como:
- Alteração de gateway padrão;
  - Alteração de subrede;
  - Alteração de domínio;
  - Alteração de servidor DHCP;
  - Alteração de servidor DNS;
  - Alteração de servidor Wins;
  - Alteração de subrede;
- 1.6.77. Possuir capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 1.6.78. Possuir capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 1.6.79. Possuir capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 1.6.80. Possuir capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 1.6.81. Possuir capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 1.6.82. Possuir capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- 1.6.83. Possuir capacidade de exportar relatórios para os seguintes tipos de arquivos: CSV, PDF;
- 1.6.84. Possuir capacidade de gerar traps SNMP para monitoramento de eventos;
- 1.6.85. Deve possuir compatibilidade com Microsoft NAP.
- 1.6.86. Possuir capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 1.6.87. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
- Nome do vírus;
  - Nome do arquivo infectado;



- Data e hora da detecção;
- Nome da máquina ou endereço ip;
- Ação realizada.

1.6.88. Possuir capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

1.6.89. Possuir capacidade de diferenciar máquinas virtuais de máquinas físicas.

## **2. Estações Windows**

### **2.1. Compatibilidade no mínimo com:**

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 / x64 SP1 ou superior.
- Microsoft Windows 8.1 Pro / Enterprise x86 / x64.
- Microsoft Windows 10 Pro / Enterprise x86 / x64.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 SP1.
- Microsoft Windows Server 2008 Standard / Enterprise x64 SP2.
- Microsoft Small Business Server 2011 Standard x64
- Microsoft Windows Server 2012 R2 Standard x64
- Microsoft Windows Server 2012 Foundation / Standard x64
- Microsoft Windows Server 2016 x64

### **2.2. Características:**

- 2.2.1. Deve prover, no mínimo, as seguintes proteções:
- 2.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 2.2.3. Antivírus de web (módulo para verificação de sites e downloads contra vírus);
- 2.2.4. Antivírus de cliente de e-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- 2.2.5. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- 2.2.6. Firewall com IDS;
- 2.2.7. Autoproteção (contra-ataques aos serviços/processos do antivírus);
- 2.2.8. Controle de dispositivos externos;
- 2.2.9. Controle de acesso a sites por categoria;
- 2.2.10. Controle de acesso a sites por horário;
- 2.2.11. Controle de acesso a sites por usuários;
- 2.2.12. Possuir a capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.2.13. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- 2.2.14. Possuir capacidade de desinstalar antivírus de outros fabricantes.
- 2.2.15. Possuir capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.
- 2.2.16. Desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

- 2.2.17. Possuir capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.2.18. Possuir capacidade de verificar somente arquivos novos e alterados;
- 2.2.19. Possuir capacidade de verificar objetos usando heurística;
- 2.2.20. Possuir capacidade de agendar uma pausa na verificação;
- 2.2.21. Deve permitir a filtragem de conteúdo de url avançada efetuando a classificação dos sites em categorias;
- 2.2.22. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve, obrigatoriamente, oferecer todas as possibilidades abaixo, para serem escolhidas pelo administrador:
- Perguntar o que fazer, ou
  - Apagar o objeto;
- 2.2.23. Possuir capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
- 2.2.24. Possuir capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- 2.2.25. Possuir capacidade de verificar links inseridos em e-mails contra phishings;
- 2.2.26. Possuir capacidade de verificar tráfego nos browsers: internet Explorer, Firefox e Chrome;
- 2.2.27. Possuir capacidade de verificação do conteúdo e anexos de e-mails usando heurística;
- 2.2.28. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve, obrigatoriamente, oferecer todas as possibilidades abaixo, para serem escolhidas pelo administrador:
- Perguntar o que fazer, ou;
  - Bloquear o e-mail;
  - Apagar o objeto;
- 2.2.29. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- 2.2.30. Possuir capacidade de filtrar anexos de e-mail, apagando-os ou renomeando os de acordo com a configuração feita pelo administrador;
- 2.2.31. Possuir capacidade de verificação de tráfego http e qualquer script do Windows script host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 2.2.32. Deve ter suporte total ao protocolo IPV6;
- 2.2.33. Possuir capacidade de alterar as portas monitoradas pelos módulos de web e e-mail;
- 2.2.34. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
- Perguntar o que fazer, ou;
  - Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou permitir acesso ao objeto;
- 2.2.35. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
- Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
  - Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

2.2.36. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

2.2.37. Deve possuir módulo que analise as ações de cada aplicação em execução no computador.

2.2.38. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

2.2.39. Deve possuir módulo de bloqueio de phishing.

2.2.40. Possuir capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.2.41. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

2.2.42. O módulo de firewall deve conter, no mínimo, dois conjuntos de regras:

- Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.2.43. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

- Discos de armazenamento locais;
- Armazenamento removível;
- Impressoras;
- CD/DVD;
- Drives de disquete;
- Modems;
- Dispositivos de fita;
- Dispositivos multifuncionais;
- Leitores de smart card;
- Wi-fi;
- Adaptadores de rede externos;
- Dispositivos MP3 ou smartphones;
- Dispositivos bluetooth;
- Câmeras e scanners.
- Permitir acesso ou bloqueio dos seguintes barramentos de conexão:
  - Infravermelho
  - Porta Serial
  - Porta paralela
  - USB
  - FireWire
  - PCMCIA

2.2.44. Possuir capacidade de liberar acesso a uma mídia removível por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

2.2.45. Possuir capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário e grupos;

2.2.46. O módulo de controle de dispositivos deverá ter a opção de cadastrar "Dispositivos Confiáveis" com intuito de permitir apenas dispositivos cadastrados pelo administrador.

2.2.47. Possuir capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo e áudio), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

2.2.48. Possuir capacidade de detectar, nativamente, ataques originados por *Ransomware*. A detecção para este tipo de malware deve basear-se não apenas nas informações do banco de dados de definições de vírus, mas também no comportamento do malware; mesmo que ainda não tenha sido desenvolvida, pelo fabricante, vacina para combater o mesmo.

### **3. Estações MAC OS x**

#### **3.1. Compatibilidade, no mínimo com:**

- Mac OS x 10.13;
- Mac OS x 10.12;
- Mac OS x 10.11;
- Mac OS x 10.10;
- Mac OS x 10.9;

#### **3.2. Características mínimas obrigatórias:**

- 3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.2.2. Possuir capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 3.2.3. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua Possuir capacidade;
- 3.2.4. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- 3.2.5. Possuir capacidade de voltar para a base de dados de vacina anterior;
- 3.2.6. Possuir capacidade de varrer a quarentena automaticamente após cada atualização de vacinas
- 3.2.7. Possuir capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.
- 3.2.8. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 3.2.9. Possuir capacidade de verificar somente arquivos novos e alterados;
- 3.2.10. Possuir capacidade de verificar objetos usando heurística;
- 3.2.11. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve, obrigatoriamente, oferecer todas as possibilidades abaixo, para serem escolhidas pelo administrador:
  - Perguntar o que fazer, ou;
  - Apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

- Caso negativo de desinfecção:
  - Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 3.2.12. Possuir capacidade de verificar arquivos de formato de email;
- 3.2.13. Deve ser possível trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, parar o antivírus e iniciar o antivírus pela linha de comando;
- 3.2.14. Possuir capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

#### **4. Estações de trabalho Linux**

##### **4.1. Compatibilidade, no mínimo com:**

###### 4.1.1. Plataformas 32-bits, no mínimo:

- Red Hat Enterprise Linux 6.7
- Red Hat Enterprise Linux 6.8
- CentOS-6.7
- CentOS-6.8
- Ubuntu Server 14.04 LTS
- Ubuntu Server 16.04 LTS
- Ubuntu Server 16.10 LTS
- Debian GNU/Linux 7.10
- Debian GNU/Linux 7.11
- Debian GNU/Linux 8.6
- Debian GNU/Linux 8.7

###### 4.1.2. Plataforma 64-bits, no mínimo:

- Red Hat Enterprise Linux 6.7;
- Red Hat Enterprise Linux 6.8;
- Red Hat Enterprise Linux 7.2;
- Red Hat Enterprise Linux 7.3;
- CentOS-6.7;
- CentOS-6.8;
- CentOS-7.2;
- CentOS-7.3;
- Ubuntu Server 14.04 LTS;
- Ubuntu Server 16.04 LTS;
- Ubuntu Server 16.10 LTS;
- Debian GNU/Linux 7.10;
- Debian GNU/Linux 7.11;
- Debian GNU/Linux 8.6;
- Debian GNU/Linux 8.7;
- OpenSUSE 42.2;
- SUSE Linux Enterprise Server 12;
- OracleLinux 7.3

## **4.2. Características:**

- 4.2.1. Deve prover, no mínimo, as seguintes proteções:
- 4.2.2. Antivírus de arquivos residente (Anti-spyware, Anti-trojan, Anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
- 4.2.3. As vacinas devem ser atualizadas pelo fabricante, no máximo, de uma em uma hora;
- 4.2.4. Possuir capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
- 4.2.5. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- 4.2.6. Gerenciamento de quarentena: quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
- 4.2.7. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; ou remoção de objetos infectados.
- 4.2.8. Em caso de erros, deve possuir a capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- 4.2.9. Possuir capacidade de verificar objetos usando heurística;
- 4.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa.

## **5. Servidores Windows**

### **5.1. Compatibilidade, no mínimo com:**

- 5.1.1 Plataforma 32-bits:
  - Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
  - Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
- 5.1.2 Plataforma 64-bits:
  - Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
  - Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
  - Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
  - Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
  - Microsoft Windows Storage Server 2008 R2;
  - Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
  - Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
  - Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
  - Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
  - Microsoft Windows Storage Server 2012 (Todas edições);

- Microsoft Windows Storage Server 2012 R2 (Todas edições);
- Microsoft Windows Hyper-V Server 2012;
- Microsoft Windows Hyper-V Server 2012 R2
- Microsoft Windows Server 2016

## **5.2 Características mínimas obrigatórias:**

- 5.2.1 Possuir antivírus de arquivos residente (Anti-spyware, Anti-Trojan, Anti-Malware,) que verifique qualquer arquivo criado, acessado ou modificado;
- 5.2.2 Possuir auto-proteção contra-ataques aos serviços/processos do antivírus;
- 5.2.3 Possuir módulo de proteção em tempo real;
- 5.2.4 Possuir capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 5.2.5 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 5.2.6 Possuir capacidade de configurar a permissão de acesso às funções do antivírus com opções, no mínimo, para as seguintes funções.
- 5.2.7 Em caso de erros, deve ter a capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- 5.2.8 Possuir capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 5.2.9 Possuir capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.
- 5.2.10 Possuir capacidade de verificar somente arquivos novos e alterados;
- 5.2.11 Possuir verificação de arquivos novos ou modificados recentemente;
- 5.2.12 Possuir verificação de setores de boot e MBR;
- 5.2.13 Possuir verificação de arquivos compactados;
- 5.2.14 Possuir verificação de processos carregados na memória;
- 5.2.15 Possuir capacidade de verificar objetos usando heurística;
- 5.2.16 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 5.2.17 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
- 5.2.18 Possuir módulo de reputação na nuvem do fabricante para detecção de novas ameaças e aplicações maliciosas.
- 5.2.19 Desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias;
- 5.2.20 Permitir a configuração de servidor proxy para conexão com a rede WAN.
- 5.2.21 Possuir capacidade de criar um arquivo DUMP com os erros;
- 5.2.22 Possuir tarefa de varredura no disco em busca de ameaças;
- 5.2.23 Possuir capacidade de reportar em tempo o número de arquivos verificados e infectados;
- 5.2.24 Possuir tarefa de atualização dos módulos do produto;
- 5.2.25 Possuir capacidade de copiar as atualizações para uma pasta externa;
- 5.2.26 Possuir capacidade de retornar a base de atualizações para uma versão anterior;
- 5.2.27 A solução deve ser gerenciada pela mesma console de gerenciamento das estações de trabalho e dispositivos móveis (Smartphones e Tablets);
- 5.2.28 Possuir log de auditoria para documentação das ações e alterações de configuração do produto;

5.2.29 Possuir capacidade de detectar, nativamente, ataques originados por *Ransomware*. A detecção para este tipo de malware deve basear-se não apenas nas informações do banco de dados de definições de vírus, mas também no comportamento do malware; mesmo que ainda não tenha sido desenvolvida, pelo fabricante, vacina para combater o mesmo.

## **6 Servidores Linux**

### **6.1 Compatibilidade, no mínimo com:**

#### 6.1.1 Plataformas 32-bits:

- Red Hat® Enterprise Linux® 6.9 Server
- CentOS-6.9
- SUSE® Linux Enterprise Server 11 SP4
- Ubuntu 16.04.2 LTS
- Ubuntu 14.04.5 LTS
- Debian GNU/Linux 7.11
- Debian GNU/Linux 8.7

#### 6.1.2 Plataforma 64-bits:

- Red Hat® Enterprise Linux® 6.9 Server
- CentOS-6.9
- SUSE® Linux Enterprise Server 11 SP4
- Ubuntu 16.04.2 LTS
- Ubuntu 14.04.5 LTS
- Debian GNU/Linux 7.11
- Debian GNU/Linux 8.7
- Red Hat® Enterprise Linux® 7.3 Server
- CentOS-7.3
- Oracle Linux 7.3
- Novell® Open Enterprise Server 2015 SP1
- SUSE® Linux Enterprise Server 12 SP2
- OpenSUSE® Leap 42.2

### **6.2 Características:**

6.2.1 Deve prover as seguintes proteções:

6.2.2 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que proteja qualquer arquivo criado, acessado ou modificado;

6.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

6.2.4 Possuir capacidade de configurar a permissão de acesso de usuários, às funções do antivírus com, no mínimo, opções para as seguintes funções:

6.2.5 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

6.2.6 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; ou remoção de objetos infectados;

6.2.7 Em caso erros, deve Possuir Possuir capacidade de criar logs automaticamente, sem necessidade de outros softwares;

6.2.8 Possuir capacidade de verificar objetos usando heurística;

6.2.9 Deve possuir módulo de administração remoto através de ferramenta nativa;

6.2.10 Deve possuir gerenciamento através de interface WEB;



## **7 Proteção para smartphones e tablets**

### **7.1 Compatibilidade:**

- Android OS 4.1-7.1.1

### **7.2 Características:**

7.2.1 Deve prover as seguintes proteções:

7.2.2 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

7.2.3 Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, bluetooth) e mensagens ems, durante sincronismo com pc e ao realizar download usando o browser;

7.2.4 Arquivos abertos no smartphone;

7.2.5 Programas instalados usando a interface do smartphone

7.2.6 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

7.2.7 Deverá isolar em área de quarentena os arquivos infectados;

7.2.8 Deverá atualizar as bases de vacinas de modo agendado;

7.2.9 Deverá bloquear spams de sms através de black lists;

7.2.10 Deverá ter função de bloqueio do aparelho caso o sim card for trocado para outro não autorizado;

7.2.11 Possuir capacidade de desativar por política:

- Câmera;

7.2.12 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

7.2.13 Possuir capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

7.2.14 Possuir capacidade de tirar fotos quando a senha for inserida incorretamente;

7.2.15 Possuir capacidade de enviar comandos remotamente de:

- Localizar;
- Bloquear.

7.2.16 Possuir capacidade de bloquear o acesso a sites phishing ou malicioso;

7.2.17 Possuir Possuir capacidade de bloquear o dispositivo quando o cartão “sim” for substituído;

7.2.18 Possuir capacidade de configurar white e blacklist de aplicativos;

7.2.19 Possuir capacidade de localizar o dispositivo quando necessário;

7.2.20 Permitir atualização das definições quando estiver em “roaming”;

7.2.21 Possuir capacidade de selecionar endereço do servidor para buscar a definição de vírus;

7.2.22 Possuir capacidade de enviar url de instalação por e-mail;

7.2.23 Possuir capacidade de fazer a instalação através de um link qrcode;

7.2.24 Possuir capacidade de executar as seguintes ações caso a desinfecção falhe:

- Deletar;
- Ignorar;
- Enviar para Quarentena;
- Perguntar ao usuário.

## **8 Gerenciamento de Dispositivos Móveis (MDM)**

### **8.1 Compatibilidade:**

- Android.
- Dispositivos com suporte ao Apple Push Notification (APNs).
- Apple iOS 9.0-10.3.

## **8.2 Características:**

- 8.2.1 Possuir capacidade de aplicar políticas de activesync através do servidor Microsoft exchange;
- 8.2.2 Possuir capacidade de ajustar as configurações de:
- Sincronização de e-mail;
  - Uso de aplicativos;
  - Senha do usuário;
- 8.2.3 Possuir capacidade de, remotamente, resetar a senha de dispositivos IOS;
- 8.2.4 Possuir capacidade de, remotamente, apagar todos os dados de dispositivos IOS;
- 8.2.5 Possuir capacidade de, remotamente, bloquear um dispositivo IOS.

## **9 Compatibilidade com Sistemas Legados:**

- 9.1 A operacionalidade da Solução em Sistemas Legados (como Windows XP) será garantida pelo uso de engines de versões anteriores buscando, se possível, o gerenciamento único.

## **IV Prazo, local e condições de entrega ou execução**

A entrega, instalação e treinamento de 20 técnicos (CeTI e Labs) será realizada em até 30 dias a partir do 1º dia útil subsequente à assinatura do Contrato. Prazo de execução (vigência do contrato): 36 meses. A instalação do Software será realizada pelos técnicos da UNITAU, com suporte da EMPRESA (veja item VII).

## **V Responsável pelo recebimento, telefone e e-mail**

O recebimento será de responsabilidade da Coordenadoria de Informática da Central de TI da UNITAU, telefone (12) 3632-3195 e (12) 3635-5244, email [infra@unitau.br](mailto:infra@unitau.br), sendo responsável o Coordenador, a Srª Edilene Dutra Moraes da Fonseca.

## **VI 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.

## **VII Obrigações da contratada**

A EMPRESA deverá informar claramente na Proposta marca e modelo da solução, sob pena de desclassificação. O suporte prestado durante a vigência contratual conforme necessidade (atualizações, configurações, webinars etc), já faz parte da solução adquirida.

**Para tanto a EMPRESA deve discriminar sites, email e telefones específicos para a CONTRATANTE acessá-la .**



Durante a instalação do Software a EMPRESA deverá prestar suporte à CONTRATANTE conforme descrito no 1º parágrafo deste item. Não sendo suficiente, é previsto o deslocamento de técnico(s) para suporte presencial.

### **VIII Qualificação técnica**

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. 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.

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

O(s) documento(s) devem 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).

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

### **IX Critério de avaliação das propostas**

O critério será o de Menor Preço Total do Item.

**Walter do Amaral Netto**  
**Analista de Sistemas Senior**  
**Central de TI = UNITAU**

### **OBSERVAÇÃO:**

**Após a reunião do Pregão, a licitante vencedora terá dois dias úteis para apresentar (por e-mail) nova planilha com os novos preços diluídos, se for o caso.**



## ANEXO II

### PROPOSTA COMERCIAL

À  
**UNIVERSIDADE DE TAUBATÉ**  
**Ref.: PREGÃO PRESENCIAL Nº 19/2018**  
**Processo PRA nº 40/18**

Apresentamos nossa proposta de preço, em 01 (uma) via, para **Aquisição de solução de segurança corporativa para endpoints, servidores e rede**, conforme especificações constantes do Anexo I, que integra o presente EDITAL, consistindo no seguinte:

| Item        | DESCRIÇÃO/MARCA  | VALOR TOTAL (R\$) |
|-------------|--|-------------------|
| <b>Lote</b> | LOTE, conforme especificações constantes no Anexo I.<br><i>Marca/Fabricante:</i> |                   |

- I. O Valor Total para o LOTE é de R\$ \_\_\_\_\_  
(\_\_\_\_\_).
- II. O prazo de validade de nossa proposta é de \_\_\_\_ (\_\_\_\_) dias corridos, obedecido o prazo mínimo do subitem 4.1.6., a contar da data prevista no subitem 1.2.2. do Edital.
- III. O prazo de instalação será conforme Anexo I – Termo de Referência e Minuta de Contrato (Anexo III).
- IV. O prazo de pagamento será conforme Anexo I – Termo de Referência e Minuta de Contrato (Anexo III).
- V. 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.



**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

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

VII. 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.

....., ..... de ..... de 2018.

-----  
(Nome Legível)

VIII. **Dados do Responsável pela Assinatura do Contrato:**

Nome completo: \_\_\_\_\_  
RG \_\_\_\_\_ CPF/MF \_\_\_\_\_  
E-mail comercial \_\_\_\_\_ E-mail pessoal \_\_\_\_\_  
Função na empresa \_\_\_\_\_

**OBSERVAÇÕES:**

**Esta Proposta Comercial (Anexo II) poderá ser preenchida pela licitante e colocada no Envelope PROPOSTA, bastando que seja aposto nesta o carimbo da licitante. Poderá, ainda, ser apresentada em papel timbrado da empresa no formato deste Anexo II.**

**Necessariamente todos os itens constantes neste modelo deverão estar presente na Proposta Comercial apresentada.**



### ANEXO III Minuta de Contrato \_\_\_\_/\_\_\_\_

**Processo:** PRA nº \_\_\_\_\_

**Licitação:** Pregão nº \_\_\_\_\_

**Regência Legal:** Lei Federal nº 10.520/02, Lei Complementar nº 123/06, com alterações da Lei Complementar nº 147/2014 e pelo Decreto Municipal de Taubaté nº 13.409/14 e subsidiariamente e no que couber pela Lei Federal nº 8.666/93.

**Objeto:** Aquisição de solução de segurança corporativa para endpoints, servidores e rede.

**Valor:** R\$ \_\_\_\_\_

**Vigência:** \_\_\_\_\_

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 seu **Magnífico Reitor Prof. Dr. José Rui Camargo**, 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 PRESENCIAL nº \_\_\_\_\_, de que trata o Processo \_\_\_\_\_, 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 10.520/02, Lei Complementar nº 123/06, com alterações da Lei Complementar nº 147/2014 e pelo Decreto Municipal de Taubaté nº 13.409/14 e subsidiariamente e no que couber pela Lei Federal nº 8.666/93 e obedecidas às disposições contidas no Edital e seus Anexos, os quais se vinculam ao presente termo, o que se segue:

#### CLÁUSULA PRIMEIRA: DO OBJETO

A CONTRATADA, na qualidade de adjudicatária do PREGÃO PRESENCIAL \_\_\_\_\_, de que trata o Processo PRA nº \_\_\_\_\_ obriga-se a cumprir o estabelecido neste instrumento contratual, que tem por objeto a **aquisição de software de solução de segurança corporativa para endpoints, servidores e**



rede Unitau (Antivírus), tudo em conformidade com as descrições, especificações e demais disposições constantes do Edital e seus anexos e Proposta Comercial, aos quais se vincula o presente instrumento de contrato, para todos os efeitos.

| Item | Descrição do Software   | UND. | Qtd.  | Valor Unitário | Valor Total |
|------|---|------|-------|----------------|-------------|
| 01   | SOLUÇÃO DE SEGURANÇA CORPORATIVA PARA ENDPOINTS, SERVIDORES E REDE. (Conforme termo de referência – ANEXO I, do Edital) | LIÇ  | 1.500 | R\$            | R\$         |

## CLÁUSULA SEGUNDA: DA EXECUÇÃO DO OBJETO

2.1. A CONTRATADA obriga-se a realizar a **entrega, o suporte de instalação e treinamento em até 30 (trinta) dias**, a contar do primeiro dia útil subsequente ao da assinatura do contrato, com prazo de vigência das **Licenças de Uso de 36 (trinta e seis) meses**, conforme Anexo I – Termo de Referência, do Edital, podendo ser prorrogado, obedecido o disposto no Art. 57 da Lei Federal nº 8.666/93, com as alterações posteriores.

## CLÁUSULA TERCEIRA – DA GARANTIA

Durante o prazo de garantia dos serviços 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 8.666/93, exigir, alternativamente e à sua escolha, o seguinte:

- atendimento ao chamado em 24 horas e solução em 72 horas, para sanar o problema detectado, sem ônus à CONTRATANTE;
- a restituição imediata da quantia paga, monetariamente atualizada, se for o caso, relativa ao serviço, que apresentar vício de qualidade, conforme inspeção realizada pela unidade requisitante da UNITAU, sem prejuízo de eventuais perdas e danos, no prazo de 10 (dez) dias, da solicitação.

## CLÁUSULA QUARTA - DO PREÇO, DO ELEMENTO ECONÔMICO E DAS CONDIÇÕES DE PAGAMENTO

4.1 A despesa decorrente desta contratação, no importe de R\$ \_\_\_\_\_ ( \_\_\_\_\_ ), e encontra-se garantida pela Nota de Empenho nº \_\_\_\_\_, que onera a dotação orçamentária nº \_\_\_\_\_, do orçamento do exercício financeiro de 2018.



4.2 A CONTRATANTE efetuará o pagamento à CONTRATADA, em até 21 (vinte e um) dias, contados da data do Ateste Definitivo 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.

§1º O requerimento de pagamento, bem como os documentos de cobrança da CONTRATADA, deverão ser entregues juntamente com a Nota Fiscal/Fatura, na Coordenadoria de Informática da Central de TI da UNITAU, telefone (12) 3632-3195 e (12) 3635-5244, e-mail [infra@unitau.br](mailto: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.

#### **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 termo de referência, neste contrato e na proposta comercial 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 – disponibilizar local adequado para a manutenção, utilizar produtos de qualidade e possuir pessoal habilidade para a prestação do serviço;





III - 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;

IV – conduzir a execução da presente avença de acordo com o Edital, Proposta Comercial de fls. 159 e de conformidade com as normas técnicas aplicáveis, observando estritamente a legislação vigente aplicável;

V – 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;

VI – 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;

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 neste instrumento contratual, 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, erro de execução, execução imperfeita, mora, inadimplemento contratual ou ainda comportar-se de modo inidôneo, cometer fraude fiscal ou constatar-se a



não veracidade de informações prestadas a Administração, poderá a CONTRATANTE aplicar à CONTRATADA, garantida a prévia e ampla defesa, as definidas nos artigos 86 e 87 da Lei Federal nº 8.666/93, e as penalidades conforme segue:

a) multa equivalente a 2% (dois por cento), sobre o valor total do contrato, por dia, pelo não cumprimento dos prazos, admitindo-se o máximo de 05 (cinco) dias, após o que poderá ser reconhecida a inexecução do ajuste;

b) 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;

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

d) multa de 5% (cinco 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 total deste ajuste, independentemente das demais sanções cabíveis;

f) multa de 10% (dez 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;

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

h) suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo de 02 (dois) anos, por inexecução do contrato total ou parcial, neste último caso quando a falta acarretar significativo prejuízo ao objeto contratado;

i) declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação perante a autoridade que aplicou a sanção, depois do ressarcimento à Administração pelos prejuízos resultantes e depois de decorrido o prazo



da sanção, aplicada com base no inciso III do artigo 87 da Lei Federal nº 8.666/93, por inexecução total do contrato ou por apresentar informação e/ou documentos falsos.

8.2 - As multas deverão ser recolhidas por meio de boleto bancário ou depósito bancário junto à Pró-reitoria de Economia e Finanças, no prazo de até 05 (cinco) dias, a contar do recebimento da notificação do setor responsável.

8.3 - Se o valor da multa aplicada não for pago será descontado da garantia contratual. Se isto não for possível, ou se este valor for superior ao da garantia prestada, a diferença será descontada dos pagamentos eventualmente devidos pela Administração, ou cobrada judicialmente, quando for o caso, conforme §§ 2º e 3º, do artigo 86, da Lei Federal nº 8.666/93.

8.4 - Para as penalidades previstas, será garantido o direito ao contraditório e à ampla defesa, que será dirigida para análise da Douta Procuradoria Jurídica.

8.5 - As penalidades serão obrigatoriamente registradas em autos próprios, e no caso de suspensão de licitar, a licitante deverá ser descredenciada, por igual período, sem prejuízo das multas previstas neste contrato e das demais cominações legais.

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

## **CLÁUSULA NONA - DA RESCISÃO CONTRATUAL**

O contrato poderá ser rescindido, na forma, com as consequências e pelos motivos previstos nos artigos 77 a 80 e 86 a 88, da Lei Federal n. 8.666/93.

§1º - A prática do disposto nos incisos I a XII e XVII do artigo 78, da Lei Federal nº 8.666/93, 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, de que trata o inciso VI do artigo em referência, desde que tal fato não acarrete prejuízo para a execução do contrato.



§2º - Ocorrendo a rescisão, com fundamento nos incisos XII a XVII do artigo 78, da Lei Federal nº 8.666/93, sem culpa da CONTRATADA, será esta ressarcida dos prejuízos que comprovadamente houver sofrido.

§3º - No que se refere ao inciso XIII do artigo 78 da Lei Federal nº 8.666/93, 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 contratantes, segundo permissivo legal contido no artigo 65, § 2º, inciso II, da Lei Federal nº 8.666/93, acrescentado pela Lei Federal nº 9.648/98.

§4º - À CONTRATANTE é reconhecido o direito de rescisão administrativa, nos termos do artigo 79 da Lei Federal nº 8.666/93, aplicando-se no que couber o disposto nos §§1º e 2º do citado artigo, bem como as regras do artigo 80 do mesmo diploma legal.

§5º - A CONTRATADA reconhece, desde já, os direitos do CONTRATANTE nos casos de rescisão administrativa, prevista no Artigo 79 da Lei Federal nº 8.666/93, e no art. 77 da Lei Estadual 6.544/89.

#### **CLÁUSULA DÉCIMA – DA IMPOSSIBILIDADE DE SUBCONTRATAÇÃO**

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 65, da Lei Federal nº 8.666/93.

#### **CLÁUSULA DÉCIMA SEGUNDA - DA LEGISLAÇÃO APLICADA**

A execução deste contrato será disciplinada pela Lei Federal nº 8.666/93, 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**

O contrato vigorará por **37 (trinta e sete) meses**, contado a partir do primeiro dia útil subsequente da assinatura do contrato, de forma a acompanhar o prazo de entrega, suporte de instalação, treinamento e o prazo da licença de uso, podendo ser prorrogado o prazo de execução, a critério exclusivo da Contratante.

## **CLÁUSULA DÉCIMA QUARTA – DA CAUÇÃO**

14.1 A CONTRATADA apresenta, neste ato, \_\_\_\_\_ importe de R\$ \_\_\_\_\_ (\_\_\_\_\_), equivalente a 5% (cinco por cento) do valor contratual, a título de caução.

14.2 A expressão monetária da caução deverá ser mantida sempre que se alterar o valor contratual, preservando-se, assim, o percentual de 5% (cinco por cento), mas seu valor será liberado integralmente apenas ao final da execução contratual satisfatória; ou pelo saldo, se houver, procedidos eventuais descontos.

## **CLÁUSULA DÉCIMA QUINTA - DA FISCALIZAÇÃO**

A execução do presente contrato será acompanhada e fiscalizada pelo setor requisitante, da CONTRATANTE, a qual anotarà 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.

15.1 A execução do objeto será acompanhada pela Coordenadora de Informática de Central de TI, Sra. Edilene Dutra Moraes da Fonseca, telefone (12) 3632-3195/ 3635-5244, e-mail: [infra@unitau.br](mailto:infra@unitau.br).

15.2 A fiscalização da execução do objeto pela CONTRATANTE não exclui nem reduz a responsabilidade da CONTRATADA pela inobservância de qualquer obrigação assumida.

## **CLÁUSULA DÉCIMA SEXTA– DO FORO**

Fica eleito o Foro da Comarca de Taubaté, do Estado de São Paulo.



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

Para firmeza e validade do que ora se estabelece, foi lavrado este Termo, em duas vias, o qual lido e achado conforme pelas partes.

Taubaté, \_\_\_\_ de \_\_\_\_\_ de 2018.

**UNIVERSIDADE DE TAUBATÉ  
CONTRATANTE**

---

**CONTRATADA**