ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
Comissão Permanente de Licitação

# EDITAL DE PREGÃO PRESENCIAL PARA REGISTRO DE PREÇOS N° 04/2010

**PROCESSO Nº 5742-18.2010.8.06.0000**

**TIPO DE LICITAÇÃO:** MENOR PREÇO GLOBAL

**SETOR SOLICITANTE:** Secretaria da Tecnologia da Informação

**DATA:** 10/09/2010

**HORA DA LICITAÇÃO: 14:00 – (horário de Brasília)**

**LOCAL:** Av. General Afonso Albuquerque Lima, s/n – Cambeba, Centro Administrativo Governador Virgílio Távora, Palácio da Justiça, Fortaleza/CE – Sala de Reuniões da Comissão Permanente de Licitações, telefones (85) 3207-7098 ou 3207-7100.

Endereço Eletrônico para pedidos de esclarecimentos: cpl.tjce@tjce.jus.br.

**PREZADOS SENHORES,**

O(A) PREGOEIRO (A) DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, com sede na Av. Gen. Afonso Albuquerque Lima s/n, - Cambeba, CEP–60822-325 torna público para conhecimento de todos os interessados, que no dia e hora acima indicados, será realizada licitação na modalidade **Pregão Presencial para Registro de Preços**, do tipo **MENOR PREÇO GLOBAL**, que será regido pela Lei Federal N. º 10.520, de 17/07/2002, pela Lei Complementar n.º 123, de 14/12/2006, pela Resolução N.º 04 de 06/03/2008 do TJCE, alterada pela Resolução N.º 08 de 09/07/2009 do TJCE, com aplicação subsidiária da Lei Federal N.º 8.666/93 e suas alterações, além das demais disposições legais aplicáveis e do disposto no presente Edital e seus Anexos.

As propostas deverão obedecer as especificações deste instrumento convocatório e anexos, que dele fazem parte integralmente.

Os envelopes contendo a "PROPOSTA COMERCIAL" e "DOCUMENTAÇÃO DE HABILITAÇÃO" serão recebidos no endereço retromencionado, na sessão pública de processamento do Pregão, após o credenciamento dos interessados que se apresentarem para participar do certame, e será conduzida pelo(a) Pregoeiro(a) com o auxílio da Equipe de Apoio.

Caso seja decretado feriado, as reuniões previstas serão realizadas no primeiro dia útil subsequente.

Este Edital está disponível gratuitamente no site: www.tjce.jus.br

**ÍNDICE GERAL**



**Integram este edital os seguintes anexos:**



## 1 OBJETO

1.1 A presente licitação tem como objeto o ***Registro de preços para aquisição de solução de segurança de TIC(Tecnologia da Informação e Comunicação), visando a interligação das unidades do Poder Judiciário, incluindo equipamentos destinados à sede do Tribunal, Fórum Clóvis Beviláqua e 209 (duzentas e nove) unidades judiciárias, bem como serviços de gerenciamento, suporte, atualização, implantação e treinamento da solução***, conforme especificado nos Anexos, partes integrantes deste Edital.

1.2 A existência de preços registrados não obriga o TJCE a firmar as contratações estimadas no ANEXO C – TERMO DE REFERÊNCIA, ficando-lhe facultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurada ao beneficiário do registro a preferência de contratação em igualdade de condições.

## 2 PRAZO DE VALIDADE

2.1 A Ata de Registro de Preços terá validade de 01(um) ano, contado a partir da data de

sua assinatura, podendo ser prorrogada nos termos legais, se ficar comprovada vantagem para Administração.

2.2 A partir da vigência da Ata de Registro de Preços, o licitante se obriga a cumprir integralmente todas as condições estabelecidas no instrumento contratual, sujeitando-se, inclusive, às penalidades pelo descumprimento de quaisquer de suas cláusulas.

2.3 As quantidades previstas no Termo de Referência – Anexo C, são estimativas máximas para o período de validade da Ata de Registro de Preços, reservando-se ao TJCE o direito de adquirir/contratar o quantitativo que julgar necessário, podendo ser parcial, integral ou mesmo abster-se de adquirir o item especificado.

## 3 CONDIÇÕES PARA PARTICIPAÇÃO

3.1 Poderá participar desta licitação toda e qualquer pessoa jurídica:

a) toda e qualquer **pessoa jurídica IDÔNEA e cuja natureza seja compatível com o objeto licitado**;

b) que seja regularmente estabelecida no País;

c) que satisfaça todas as exigências, especificações e normas contidas neste Edital e em seus Anexos;

3.2 **É vedada a participação de interessados:**

3.2.1 Que estejam reunidos em consórcio, coligação ou grupos de empresas, que tenham em comum com uma ou mais empresas participantes deste processo licitatório, um ou mais sócios quotistas ou membros de diretoria;

3.2.2 Que estejam cumprindo pena de suspensão temporária de participar de licitações e impedimento de contratar com a Administração Pública;

3.2.3 Que estejam declarados inidôneos pela Administração Pública;

3.2.4 Estrangeiros que não funcionem no País;

3.2.5 Que estejam sob processo de recuperação judicial ou extrajudicial, concordata, falência, dissolução, fusão, cisão, incorporação, liquidação ou esteja suspensa de licitar;

3.2.6 **Servidor(es) dos órgãos e entidades da Administração Pública Estadual, inclusive Fundações instituídas e/ou mantidas pelo Poder Público, como licitante, direta ou indiretamente, por si ou por interposta pessoa, do presente processo licitatório;**

3.3 A participação na licitação implica automaticamente a aceitação integral dos termos deste Edital e seus Anexos e legislação aplicável.

3.4 A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas neste edital.

## 4 CREDENCIAMENTO DOS REPRESENTANTES.

4.1 A abertura da presente licitação dar-se-á em sessão pública, dirigida por um(a) Pregoeiro(a), a ser realizada conforme indicado abaixo, de acordo com a legislação mencionada no preâmbulo e o conteúdo deste Edital.

4.2 Cada licitante deverá apresentar **FICHA DE CREDENCIAMENTO conforme Anexo A** deste edital, por meio de seu representante credenciado.

4.3 No local, data e hora indicados no preâmbulo deste edital e na presença do(a) Pregoeiro(a) e da Equipe de Apoio, será realizado o credenciamento do(s) representante(s) do(s) licitante(s). Para tanto será indispensável a apresentação dos seguintes documentos:

a) Documento oficial de identidade.

b) Ficha de credenciamento devidamente preenchida, em papel timbrado do licitante, conforme modelo do **ANEXO A** deste edital.

c) Tratando-se de representante legal, o estatuto social, contrato social ou outro instrumento de registro comercial, tratando-se de sociedades civis, o ato constitutivo registrado no Cartório de Registro Civil de Pessoas Jurídicas, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura.

d) Tratando-se de procurador, o instrumento de procuração pública ou particular com firma

reconhecida, no qual constem poderes específicos para formular lances, negociar preço, interpor recursos e desistir de sua interposição e praticar todos os demais atos pertinentes ao certame, acompanhado do correspondente documento que comprove os poderes do mandante para a outorga (contrato social ou documento similar).

4.4 Caso a procuração seja particular, deverá ter firma reconhecida e estar acompanhada dos documentos comprobatórios dos poderes de outorgante.

4.5 Somente a pessoa credenciada nos termos do item anterior terá poderes para a formulação de propostas verbais e para a prática de todos os demais atos inerentes ao certame.

4.6 Ficará impedido de formular lances verbais, o credenciado cuja procuração não contenha autorização expressa para este fim.

4.7 A não apresentação ou incorreção de qualquer documento de credenciamento, impossibilitará o representante de formular lances no certame e praticar todos os demais atos inerentes ao Certame.

4.8 O credenciado deverá ter amplo conhecimento do teor da proposta apresentada, em todos os seus itens, a fim de que o licitante se faça representar, legitimamente, em eventuais negociações entre as partes, evitando com isso a interrupção da sessão para contatos externos visando o esclarecimento de dúvidas sobre o teor da mesma, ficando, todavia, os casos excepcionais para serem avaliados pelo Pregoeiro.

4.9 Cada licitante credenciará apenas um representante que será o único admitido a intervir nas fases do procedimento licitatório e a responder por todos os atos e efeitos previstos neste Edital, por sua representada.

4.10 Não será admitida a participação de um mesmo representante para mais de uma empresa licitante.

## 5 DA FORMA DE APRESENTAÇÃO DA DECLARAÇÃO DE PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO, DA PROPOSTA E DOS DOCUMENTOS.

5.1 A declaração de pleno atendimento aos requisitos de habilitação deverá ser apresentada fora dos Envelopes n.ºs 1 e 2 e de acordo com modelo estabelecido no **ANEXO B** ao Edital.

5.2 No dia, hora e local designado neste edital de Pregão, na presença dos representantes dos licitantes, devidamente credenciados e demais pessoas que queiram assistir ao ato, o Pregoeiro receberá dos representantes credenciados, em envelopes distintos, devidamente fechados e rubricados nos fechos, as propostas de preço e a documentação exigida para a habilitação dos licitantes, registrando em ata os participantes do certame.

5.3 A "PROPOSTA" e a "DOCUMENTAÇÃO", deverão ser apresentados, separadamente, em 02 envelopes fechados e indevassáveis, contendo em sua parte externa, além do nome da proponente, os seguintes dizeres:

**AO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ**
**ENVELOPE Nº 1 – PROPOSTA**
**PREGÃO PRESENCIAL N.º ___/2010 – TJCE**
**PROPONENTE:**

**AO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ**
**ENVELOPE Nº 2 – DOCUMENTAÇÃO**
**PREGÃO PRESENCIAL N.º ___/2010 – TJCE**
**PROPONENTE:**

5.4 A proposta deverá ser elaborada em papel timbrado do licitante e redigida em língua portuguesa, com suas páginas numeradas sequencialmente, rubricadas, sem rasuras, emendas, borrões ou entrelinhas e ser datada e assinada pelo titular do licitante ou representante legal (titular ou procurador), juntando-se cópia da procuração.

5.5 Os documentos, deverão ser apresentados em original, por qualquer processo de cópia autenticada por tabelião de notas, ou via internet.

## 6 DO CONTEÚDO DO ENVELOPE "PROPOSTA"

6.1 A "PROPOSTA" deverá conter os seguintes elementos:

a) nome, endereço, CNPJ e inscrição estadual/municipal;

b) número do **processo** e do **Pregão**;

c) descrição do objeto da presente licitação, em conformidade com a planilha de composição de custos do **Anexo D** e demais especificações nos anexos deste Edital;

d) Preço unitário e global, em moeda corrente nacional (real), sendo este último por extenso, incluindo todos os custos diretos e indiretos, incidentes sobre o objeto. Caso haja divergência entre o valor numérico e por extenso, prevalecerá este último;

e) prazo de validade da proposta de, no mínimo, 60 (sessenta) dias a ser contado a partir da sua emissão;

f) declaração de que cumpre o Acordo de Nível de Serviço (ANS) especificado no item 3.8.4 do Anexo C;

g) declaração, **SE COUBER**, de que é considerada **MICROEMPRESA OU EMPRESA DE PEQUENO PORTE**, conforme incisos I e II, do artigo 3º, da Lei Complementar n.º 123, de 14/12/2006, e que não se encontra alcançada por qualquer das hipóteses descritas no § 4º, do artigo 3º, da Lei Complementar n.º 123, de 14/12/2006, **e, ainda, que tem interesse em usar a prerrogativa do desempate** instituído no §1º, do artigo 44 da referida Lei.

6.2 Os proponentes deverão anexar na proposta de preços, **SOB PENA DE DESCLASSIFICAÇÃO**:

6.2.1 Uma planilha para comprovação dos requisitos técnicos, conforme exigido no item 9 - MODELO DE PLANILHA DE REQUISITOS TÉCNICOS do **Anexo C d**este edital, demonstrando o atendimento dos requisitos técnicos para os produtos solicitados (Soluções de Firewall/VPN, IPS e soluções de gerenciamento e correlação de eventos – CÓDIGOS 01 A 07), contemplando cada subitem especificado no item 3 do Anexo C – ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS E SERVIÇOS;

6.2.2 Todas as exigências deverão ser comprovadas conforme especificado no subitem 9.2 do **Anexo C** deste edital.

6.2.3 Ficha de dados da pessoa que irá assinar o Contrato, ou equivalente, caso o licitante seja declarado vencedor do certame, conforme modelo constante no **ANEXO H.**

## 7 DO CONTEÚDO DO ENVELOPE "DOCUMENTAÇÃO DE HABILITAÇÃO"

7.1 Para habilitação, os interessados deverão apresentar na sessão de recebimento da proposta e documentação, em uma via, os documentos abaixo discriminados precedidos de uma folha de índice, com todas as folhas numeradas, rubricadas e indicação do número total de folhas, em envelope fechado.

7.1.1 *Certificado de Registro Cadastral – CRC* expedido pela Secretaria de Planejamento e Gestão do Estado do Ceará - SEPLAG, ou documento similar expedido pelo órgão competente do domicílio fiscal do licitante, que comprove estar o licitante cadastrado para o exercício dos serviços, objeto deste certame;

7.1.1.1 *A Comissão verificará a situação do licitante no CRC.* Caso o mesmo esteja com algum documento vencido, deverá apresentá-lo juntamente com os documentos de habilitação, sob pena de inabilitação.

7.1.2 *Certidão Negativa de Débitos para com a Previdência Social* – CND, dentro do prazo de validade;

7.1.3 *Certidão Negativa de Débitos para com o FGTS*, emitido pela Caixa Econômica Federal, dentro do prazo de validade;

7.1.4 *Ato constitutivo, estatuto ou contrato social em vigor e a última alteração ou a última alteração consolidada, devidamente registrado*, em se tratando de sociedades empresariais e, no caso de sociedades por ações, acompanhados de documentos de eleição de seus administradores; ou inscrição do ato constitutivo, no caso de sociedades simples, acompanhada de prova de Diretoria em exercício;

## 7.2 QUALIFICAÇÃO ECONÔMICO FINANCEIRA

7.2.1 *Balanço Patrimonial e demonstrações contábeis do último exercício,* já exigíveis, e apresentados na forma da Lei, devidamente registrados na Junta Comercial, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de três meses da data da apresentação da proposta;

7.2.2 *A comprovação da boa situação financeira* do licitante será atestada por documento assinado por profissional legalmente habilitado, demonstrando que a empresa apresenta "Índice de Liquidez Geral (ILG)" maior ou igual 1,2 (um vírgula dois) calculado pela fórmula abaixo:

$$\textbf{ILG} = \frac{\textbf{Ativo Circulante + Realizável a Longo Prazo}}{\textbf{Passivo Circulante + Exigível a Longo Prazo}}$$

7.2.3 *Certidão Negativa de falência ou concordata* expedida pelo distribuidor judicial, justiça ordinária, dentro do prazo de validade expresso na própria certidão.

7.2.4 A proponente deverá comprovar por meio da Certidão Simplificada da Junta Comercial, que possui na data da publicação deste Edital, Capital Social Mínimo no valor de R$ 199.500,00 (cento e noventa e nove mil e quinhentos reais).

## 7.3 QUALIFICAÇÃO TÉCNICA

7.3.1 A LICITANTE deverá anexar declaração dos fabricantes dos componentes envolvidos na solução ofertada, dirigida especificamente ao Tribunal de Justiça e em relação a este processo licitatório, emitida em papel timbrado e devidamente assinada, atestando que a LICITANTE está apta para revender, instalar e configurar os componentes ofertados.

7.3.2 Caso a LICITANTE seja fabricante dos produtos ofertados deverá anexar TERMO DE ATESTADO DE FABRICAÇÃO, conforme solicitado no ANEXO G. Caso a LICITANTE não seja fabricante dos produtos ofertados deverá anexar DOCUMENTO COMPROBATÓRIO DO FABRICANTE a ser fornecido pelos fabricantes dos produtos ofertados, conforme solicitado no ANEXO F.

7.3.3 A LICITANTE deverá comprovar que possui em seus quadros técnicos profissional certificado pelo fabricante na solução de Firewall/VPN/IPS proposta (Será aceita certificação do fabricante que contemple as tecnologias envolvidas, não focada especificamente em produtos). Será aceito como comprovação do vínculo do profissional a cópia da GFIP do mês anterior à publicação deste Edital, para o caso de funcionários, ou Contrato Social, para o caso de sócios.

7.3.4 A LICITANTE deverá comprovar que possui portal para abertura dos incidentes. Deverá ser fornecida URL de acesso ao portal, bem como credenciais de acesso ao sistema, que será averiguado na fase de pré-qualificação por meio de simulações.

7.3.5 A LICITANTE deverá apresentar atestado de capacidade técnica, que demonstre sua experiência no fornecimento de equipamento ou prestação de serviços gerenciados, contemplando Firewall/VPN em alta disponibilidade, do mesmo fabricante da solução proposta, protegendo ambiente com pelo menos 500 estações de trabalho ou pelo menos 100 firewalls.

7.3.6 A LICITANTE deverá apresentar atestado de capacidade técnica, que demonstre sua experiência no fornecimento de equipamento ou prestação de serviços gerenciados, contemplando IDS ou IPS, do mesmo fabricante da solução proposta, protegendo ambiente com pelo menos 500 estações de trabalho.

7.3.7 A LICITANTE deverá apresentar atestado de capacidade técnica, que demonstre sua experiência no fornecimento de software de correlação de eventos, do mesmo fabricante da solução proposta.

7.3.8 Alternativamente serão aceitos atestados de capacidade técnica contemplando experiência da LICITANTE nas soluções de Firewall/VPN e IDS/IPS que contemple equipamentos de fabricantes distintos do proposto. Nesse caso, obrigatoriamente, além do atestado deverá ser anexado:

7.3.8.1 Comprovação, por parte da LICITANTE, da contratação dos serviços profissionais do fabricante para implantação e configuração de toda a solução proposta para os produtos especificados no CÓDIGO 01, 02, 04, 05 e 06. Na execução dos serviços deverão ser utilizados membros do quadro técnico permanente do fabricante, sendo vedada qualquer subcontratação neste sentido.

7.3.9 Alternativamente serão aceitos atestados de capacidade técnica contemplando experiência da LICITANTE nas soluções de Correlação de Eventos que contemple softwares de fabricantes distintos do proposto. Nesse caso, obrigatoriamente, além do atestado deverá ser anexado:

7.3.9.1 Comprovação, por parte da LICITANTE, da contratação dos serviços profissionais do fabricante para implantação e configuração de toda a solução proposta para os produtos especificados no CÓDIGO 07. Na execução dos serviços deverão ser utilizados membros do quadro técnico permanente do fabricante, sendo vedada qualquer subcontratação neste sentido.

7.3.10 A LICITANTE deverá apresentar declaração de que disponibilizará estrutura própria na cidade de Fortaleza para realização dos serviços de operação gerenciada com, no mínimo, 1(um) técnico de segundo nível, com as qualificações exigidas no item 3.8.6.1.2 deste Termo.

7.3.11 A LICITANTE deverá comprovar possuir como atividade a prestação de serviços de gerenciamento de segurança da informação. A comprovação dar-se-á por meio de fornecimento de atestados de capacidade técnica emitido por empresa pública ou privada.

7.3.12 A LICITANTE deverá apresentar declaração indicando a empresa responsável pelos serviços de assistência técnica e suporte técnico (fabricante ou autorizada);

7.3.13 A empresa indicada para prestar o serviço de assistência técnica deve possuir, pelo menos, 1 (um) técnico certificado pelo fabricante com habilitação para prestar os serviços técnicos nos equipamentos apresentados. Caso a assistência técnica não seja prestada diretamente pelo fabricante através de seus funcionários deverá ser anexado à proposta o TERMO DE ASSISTÊNCIA TÉCNICA, conforme ANEXO E.

7.3.14 Em atendimento ao disposto no inciso V do Art. 27 da Lei 8.666/93, a empresa deverá apresentar declaração expressa de que não existe na empresa, trabalhador nas situações previstas no inciso XXXIII do Art. 7 da Constituição Federal, conforme modelo do ANEXO I – Declaração de Inexistência de Emprego de Menor.

## 7.4 ORIENTAÇÕES SOBRE A FASE DE HABILITAÇÃO

7.4.1 Os documentos apresentados deverão ser, obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos para matriz e todas as filiais(por exemplo: os atestados de capacidade técnica solicitados). O contrato, ou instrumento equivalente, será celebrado com a sede que apresentou a documentação;

7.4.2 A documentação apresentada em qualquer processo de fotocópia deverá ser, obrigatoriamente, autenticada em Cartório. Caso a documentação tenha sido emitida via Internet, que esteja condicionada à verificação de sua autenticidade pelo Pregoeiro, só será aceita após o cumprimento desta formalidade;

7.4.3 Os documentos deverão ser apresentados dentro do prazo de validade. Na hipótese de no documento não constar expressamente o prazo de sua validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre a validade do mesmo. Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de **90(noventa) dias** a partir da data de sua emissão, quando se tratar de documentação referente à habilitação fiscal e econômico-financeira.

7.5 Somente serão aceitos documentos acondicionados no envelope 2, não sendo admitido posteriormente, o recebimento pelo Pregoeiro e Equipe de Apoio de qualquer outro documento, nem permitido ao licitante fazer qualquer adendo aos documentos entregues aos mesmos.

7.6 Caso haja inserção de original de documento junto com as cópias autenticadas, o

mesmo constará do processo e não poderá ser devolvido ao licitante.

7.7 As certidões de comprovação de regularidade, bem como, as de falência exigidas neste Edital, que não apresentarem, expressamente, seu período de validade, deverão ter sido emitidas nos 90(noventa) dias até a data marcada para o recebimento dos envelopes.

7.8 O Pregoeiro poderá solicitar, também, originais de documentos já autenticados, para fins de verificação, sendo o licitante obrigado a apresentá-los no prazo determinado na solicitação, sob pena, de não o fazendo, ser considerado inabilitado.

7.9 Caso a solicitação constante do item anterior seja feita durante a sessão de Habilitação, a mesma deverá constar em ATA, nela constando o prazo máximo referido.

7.10 O Pregoeiro e Equipe de Apoio não autenticarão cópias de documentos exigidos neste Edital.

7.11 A falta de credenciamento ou da entrega da declaração de habilitação por parte do licitante, importa na preclusão do direito de participar das fases subsequentes.

7.12 Constatando o atendimento das exigências previstas no Edital, o licitante será declarado vencedor do objeto da licitação pelo próprio Pregoeiro.

7.13 Se o licitante desatender às exigências previstas neste Item, o Pregoeiro examinará a oferta subsequente na ordem de classificação, verificando a sua aceitabilidade e procedendo a sua habilitação, repetindo esse procedimento sucessivamente, se for necessário, até a apuração de uma proposta que atenda ao Edital, sendo o respectivo licitante declarado vencedor.

7.14 É facultado ao Pregoeiro ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documentos ou informação que deverá constar originariamente da proposta.

## 8 DO PROCEDIMENTO E DO JULGAMENTO

8.1 No horário e local indicados no preâmbulo deste edital, será aberta a sessão de processamento do Pregão, iniciando-se com o recebimento das fichas de credenciamento dos interessados em participar do certame, com duração mínima de 15(quinze) minutos.

8.1.1 O tempo a que se refere o subitem anterior não é de **tolerância** para a abertura da sessão, e sim para o **período de credenciamento**.

8.2 Após o credenciamento, os licitantes entregarão ao Pregoeiro a declaração de pleno atendimento aos requisitos de habilitação, de acordo com o estabelecido no ANEXO B do Edital e, em envelopes separados, a proposta de preços e os documentos de habilitação.

8.3 A análise das propostas pelo Pregoeiro visará ao atendimento das condições estabelecidas neste Edital e seus anexos, sendo desclassificadas as propostas:

a) cujo objeto não atenda as especificações, prazos e condições fixados no Edital;

b) serão desconsideradas ofertas ou vantagens baseadas nas propostas dos demais licitantes;

8.4 As propostas não desclassificadas serão selecionadas para a etapa de lances, com observância dos seguintes critérios:

a)Seleção da proposta de menor preço e as demais com preços até 10% superiores àquela;

b)Não havendo pelo menos 3 (três) preços na condição definida na alínea anterior, serão selecionadas as propostas que apresentarem os menores preços, até o máximo de 3 (três). No caso de empate nos preços, serão admitidas todas as propostas empatadas, independentemente do número de licitantes.

c)O Pregoeiro convidará individualmente os autores das propostas selecionadas a formular lances de forma sequencial, a partir do autor da proposta de maior preço e os demais em ordem decrescente de valor, decidindo-se por meio de sorteio para o início da oferta de lance no caso de empate de preços.

d)Os lances deverão ser formulados em valores distintos e decrescentes, inferiores à proposta de menor preço.

e)A etapa de lances será considerada encerrada quando todos os participantes dessa etapa

declinarem da formulação de lances.

f)Encerrada a etapa de lances, serão classificadas as propostas selecionadas e não selecionadas para a etapa de lances, na ordem crescente dos valores, considerando-se para as selecionadas o último preço ofertado.

g)O Pregoeiro poderá negociar com o autor da oferta de menor valor com vistas à redução do preço.

h)Após a negociação, se houver, o Pregoeiro examinará a aceitabilidade do menor preço, decidindo motivadamente a respeito.

i)Sendo aceitável a proposta final classificada em primeiro lugar, será aberto o envelope contendo a documentação de habilitação do licitante que a formulou, para confirmação das suas condições de habilitação.

j)Constatado o atendimento das exigências fixadas neste edital, o Pregoeiro declarará o licitante vencedor, e lhe adjudicará o objeto do certame.

k)Se a oferta não for aceitável, ou se o licitante desatender as exigências para a habilitação, o Pregoeiro examinará a oferta subsequente de menor preço, negociará com o seu autor, decidirá sobre a sua aceitabilidade e, em caso positivo, verificará as condições de habilitação e assim sucessivamente, até a apuração de uma oferta aceitável cujo proponente atenda os requisitos de habilitação, caso em que será declarado vencedor.

8.5 Será observado no critério de julgamento o que preceitua o art. 44, §§ 1º e 2º da Lei Complementar nº 123, de 14 de dezembro de 2006, sendo assegurada às microempresas e empresas de pequeno porte a oportunidade de se utilizarem do direito de preferência.

8.5.1 Encerrada definitivamente a disputa, o Pregoeiro examinará o porte da empresa arrematante, e, se esta não for Microempresa ou Empresa de Pequeno Porte, o Pregoeiro, em ordem sequencial, provocará todos que forem ME e EPP, e cujos valores contenham até 5% (cinco por cento) de diferença do arrematante, para, no prazo máximo de **5(cinco) minutos,** utilizando-se do DIREITO DE PREFERÊNCIA, cobrir a proposta do arrematante, sob pena de preclusão, de acordo com o parágrafo 3º do Art. 45 da Lei Complementar nº 123/2006.

8.5.2 Se a primeira empresa consultada pelo Pregoeiro, que seja ME ou EPP fechar negócio, a disputa será encerrada; se não, o Pregoeiro consultará as demais em ordem sequencial.

8.5.3 Se nenhuma empresa que se encontre nas condições determinadas pela LC nº 123/06 fechar negócio, o Pregoeiro considerará a proposta do arrematante.

8.6 O licitante deverá observar o capital mínimo exigido neste edital.

8.7 Quando o proponente vencedor não apresentar situação regular, no ato da assinatura da Ata de Registro de Preços, do contrato ou instrumento equivalente, será convocado outro licitante, observado a ordem de classificação, para celebrar o contrato, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

8.8 Se o licitante vencedor recusar-se, injustificadamente, a assinar a Ata de Registro de Preços, contrato ou instrumento equivalente, consequentemente não cumprir as obrigações contraídas, será aplicada a regra estabelecida no subitem anterior.

8.9 Da sessão será lavrada ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

## 9 DOS ESCLARECIMENTOS, DA IMPUGNAÇÃO, DO RECURSO, DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

9.1 Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao Pregoeiro via *e-mail* citado no preâmbulo deste edital ou por meio de *fax símile*, até 03(três) dias úteis anteriores a data fixada para a abertura da sessão pública. Não serão aceitos comunicados verbais, nem pedidos de esclarecimentos formulados após o prazo aqui estabelecido.

9.2 Até 02(dois) dias úteis antes da data fixada para a abertura da sessão pública, qualquer pessoa poderá impugnar o ato convocatório do pregão.

9.2.1 Caberá ao Pregoeiro, auxiliado pela área interessada, quando for o caso, decidir

sobre a petição no prazo de 24(vinte e quatro) horas.

9.2.2 Acolhida a impugnação contra o ato convocatório, será definida e publicada nova data para realização do certame.

9.3 Declarado o vencedor, qualquer licitante poderá manifestar, imediata e motivadamente, a intenção de recorrer contra qualquer manifestação do Pregoeiro, com registro em Ata da síntese dos respectivos fundamentos, desde que munido de procuração com poderes específicos para tal, e terá o prazo de 03(três) dias para trazer as razões escritas, ficando os demais licitantes desde logo intimados a apresentar as contra-razões no mesmo prazo, que começará a correr do término do prazo da recorrente, sendo-lhe assegurada vista imediata dos autos.

9.3.1 As impugnações e os recursos devem ser protocolizados na sede do Tribunal de Justiça do Estado do Ceará – Palácio da Justiça, Av. General Afonso Albuquerque Lima, s/n, Bairro: Cambeba – Centro Administrativo Governador Virgílio Távora, Fortaleza-CE, não sendo aceitas impugnações e recursos interpostos via fax-símile, e-mail ou telegrama.

9.4 A ausência de manifestação imediata e motivada do licitante importará a decadência do direito de recurso e o encaminhamento do processo à autoridade competente para a homologação e adjudicação.

9.5 Interposto o recurso, o Pregoeiro poderá reconsiderar a sua decisão ou encaminhá-lo devidamente informado à autoridade competente.

9.6 Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto do certame ao licitante vencedor e homologará o procedimento.

## 10 CONDIÇÕES DE PAGAMENTO

10.1 Os pagamentos referentes aos serviços serão realizados por meio de depósito bancário nas agências do Bradesco S.A, devendo as Faturas/Notas Fiscais serem entregues até o dia 10 (dez) do mês subsequente à sua efetiva prestação. As Faturas/Notas Fiscais deverão ser pagas, sem quaisquer acréscimo e atualização monetária, até o último dia útil do referido mês, devidamente atestado pelo Setor competente deste Tribunal de Justiça. Essas Notas Fiscais/Faturas deverão ser emitidas em nome do Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário – FERMOJU, CNPJ N.º 41.655.846/0001-47.

10.2 Os pagamentos referentes aos equipamentos serão realizados por meio de depósito bancário nas agências do Bradesco S.A, devendo as Faturas/Notas Fiscais serem entregues até o dia 10 (dez) do mês subsequente à emissão do Termo de Recebimento definitivo. As Faturas/Notas Fiscais deverão ser pagas, sem quaisquer acréscimo e atualização monetária, até o último dia útil do referido mês, devidamente atestado pelo Setor competente deste Tribunal de Justiça. Essas Notas Fiscais/Faturas deverão ser emitidas em nome do Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário – FERMOJU, CNPJ N.º 41.655.846/0001-47.

10.3 As faturas para pagamento deverão vir acompanhadas da comprovação de situação regular perante o FGTS, INSS, Fazenda Federal e Fazenda Estadual.

## 11 DO REAJUSTAMENTO DO PREÇO

11.1 Reajustamento: Os preços oferecidos serão irreajustáveis;

11.2 Os recursos financeiros correrão por conta do Fundo Especial de Reaparelhamento e Modernização Judiciária – FERMOJU, tendo como Fonte dos recursos os Recursos Próprios.

11.3 Os contratos resultantes da Ata de Registro de Preços poderão ser reajustados somente depois de 1(um) ano, a contar da data de assinatura do contrato. Quando da solicitação de reajuste de preço, será utilizado como base na variação do IPC-A calculada pela Instituto Brasileiro de Geografia e Estatística. Em caso da extinção do referido índice, o Tribunal fará a opção do índice que servirá de reajuste. Ficará a critério do Tribunal de

Justiça, concordar ou não com o reajuste de preço.

## 12 DA ASSINATURA DA ATA DE REGISTRO DE PREÇOS

12.1 Os licitantes classificados deverão assinar a Ata de Registro de Preços, conforme minuta constante no ANEXO J, no prazo de cinco dias úteis, contados da data do recebimento da convocação.

12.1.1 A Ata de Registro de Preços deverá ser assinada na Central de Contratos e Convênios do TJCE – Palácio da Justiça, 2º andar - Cambeba- Fortaleza-Ce., por representante legal, diretor ou sócio da empresa, devidamente acompanhado de procuração ou contrato social e cédula de identificação.

12.2 O prazo para a assinatura da Ata de Registro de Preços poderá ser prorrogado por uma única vez, desde que solicitado formalmente durante o prazo transcurso e ocorra motivo justificado e aceito pela Administração.

12.3 A existência de preços registrados não vincula a Administração a firmar contratações que deles possam advir, não gerando aos licitantes direito a indenizações de quaisquer espécies.

12.4 Respeitada a legislação pertinente às licitações e ao registro de preços, fica facultada à Administração a realização de certame específico para a aquisição pretendida, assegurando-se ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

## 13 CONTRATAÇÃO DOS SERVIÇOS E FORNECIMENTOS

13.1 Durante o prazo de validade do registro, o licitante detentor poderá ser convidado a firmar contratações de prestações de serviços, observadas as condições fixadas neste Edital e nas determinações contidas na legislação pertinente.

13.2 Aplica-se às contratações decorrentes de registro de preços o disposto no Capítulo III da Lei Federal n.º 8.666/93, com suas respectivas alterações posteriores, no que couber.

13.3 Na hipótese de o licitante primeiro classificado ter seu registro cancelado e/ou não firmar a contratação no prazo e condições estabelecidos, poderá ser firmada contratação com o segundo classificado, desde que nas mesmas condições propostas pela primeira e atendidas as especificações e prazos exigidos neste Edital.

13.4 A contratação resultante do objeto deste Edital reger-se-á ainda pelas normas fixadas pelo Código de Defesa do Consumidor, Lei n. 8.078, de 11.09.90.

13.5 A contratação decorrente desta licitação terá o termo contratual que deverá ser assinado pelas partes, no prazo de **05(cinco) dias** úteis a partir da data da convocação encaminhado ao licitante vencedor do certame.

13.6 Consideram-se como parte integrante do contrato, os termos da proposta vencedora e seus anexos, os documentos de habilitação, bem como os demais elementos concernentes à licitação, que serviram de base ao processo licitatório;

13.7 O prazo de convocação a que se refere o subitem 13.6, poderá ter uma única prorrogação com o mesmo prazo, quando solicitado pelo licitante, e desde que ocorra motivo justificado e aceito pela Administração;

13.8 Se, por ocasião da formalização do contrato, as certidões de regularidade de débito do Detentor da Ata de Registro de Preços perante o Sistema de Seguridade Social (INSS), o Fundo de Garantia por Tempo de Serviço (FGTS), a Fazenda Nacional e Estadual, estiverem com os prazos de validade vencidos, o órgão licitante verificará a situação por meio eletrônico hábil de informações, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios, salvo impossibilidade devidamente justificada;

13.9 Se não for possível atualizá-los por meio eletrônico hábil de informações o Detentor da Ata de Registro de Preços será notificado para, no prazo de 02(dois) dias úteis, comprovar a sua situação de regularidade de que trata o subitem supra, mediante a apresentação das certidões respectivas, com prazos de validade em vigência, sob pena de a contratação não se realizar;

13.10 Quando o Detentor da Ata de Registro de Preços, convocado dentro do prazo

de validade de sua proposta, não apresentar a situação regular de habilitação exigida neste edital ou se recusar a assinar o contrato, será convocado outro licitante na ordem de classificação das ofertas, e assim sucessivamente, com vistas à celebração da contratação;

13.11 Para fins de contratação, o licitante vencedor que recolha encargos sociais ou tributos diferenciados, deverá informar ao TJCE quando da assinatura do mesmo.

13.12 A duração do Contrato será 39 (trinta e nove) meses, podendo ser prorrogado, nos termos da Lei, até o limite de 60 (sessenta) meses.

## 14 DA GARANTIA CONTRATUAL

14.1 O Detentor da Ata de Registro de Preços deverá oferecer a título de garantia no ato da assinatura do contrato, e conforme o art. 56, da Lei nº 8.666/93 e suas alterações posteriores, 5%(cinco por cento) do valor a ser contratado, atualizado, podendo optar por uma das modalidades seguintes:

a) Caução em dinheiro ou título da dívida pública, vedada a prestação de garantia mediante Título da Dívida Agrária – TDA. No caso de opção pela Garantia em Título da Dívida Pública, tais títulos deverão ser acompanhados de documento emitido pela SECRETARIA DO TESOUSO NACIONAL, no qual este atestará a sua validade, exequidade e avaliação de resgate atual;

b) Fiança Bancária;

c) Seguro–Garantia.

14.2 O Proponente se obriga a prestar garantia complementar no caso de acréscimo no valor contratual.

14.3 A Garantia prestada será liberada ou restituída após a execução do contrato, e, quando em dinheiro corrigida monetariamente.

## 15 DAS SANÇÕES ADMINISTRATIVAS

15.1 A recusa sem justificativa plausível em assinar a Ata de Registro de Preços dentro do prazo estabelecido pelo Tribunal de Justiça do Estado do Ceará, caracteriza o descumprimento total das obrigações assumidas e o fornecedor será considerado inadimplente, estando sujeito à multa prevista no subitem 15.2. deste Edital.

15.2 Caso o Detentor da Ata de Registro de Preços se recuse a assinar o contrato ou instrumento equivalente dentro do prazo de validade da Ata ou convidado a fazê-lo não atenda no prazo fixado, garantida prévia e fundamentada defesa, será considerado inadimplente e estará sujeito às seguintes cominações, independentemente de outras sanções previstas na Lei 8.666/93 e suas alterações:

15.2.1. Será aplicada ao licitante detentor da Ata de Registro de Preço, caso este se recuse a executar o(s) objeto(s) a ele vinculado(s), dentro do prazo previsto, multa correspondente a 0,33% (trinta e três centésimos por cento) por dia, calculada sobre o valor correspondente ao objeto não executado, até o limite de 10% (dez por cento) desse valor, e o impedimento para contratar com Órgãos/Entidades do Estado do Ceará por período de até 05(cinco) anos;

15.2.2. Caberá, também, penalidade de multa nos seguintes casos e percentuais:

15.2.2.1. Havendo atraso na entrega dos equipamentos, multa de 0,5% por dia útil, até o máximo admitido de 5%, calculada sobre o valor do contrato;

15.2.2.2. Havendo atraso, durante a vigência da garantia e manutenção, no atendimento de chamados técnicos, multa no percentual de 0,1% por hora útil de atraso, calculada sobre o valor do contrato, limitada a 5%.

15.2.3. Caberá, ainda, a aplicação das multas previstas no item 3.8.4 do Termo de Referência, no caso de não atendimento dos prazos previstos para os serviços de operação gerenciada.

15.3 Suspensão do direito de licitar pelo prazo máximo de 05(cinco) anos;

15.4 As multas aplicadas serão descontadas de qualquer crédito existente da CONTRATADA ou cobradas judicialmente e terão como base de cálculo o cronograma

inicial do fornecimento.

15.5 Nenhuma sanção será aplicada sem o devido processo administrativo, que prevê defesa prévia do interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vista ao processo.

## 16 RECURSOS FINANCEIROS

16.1 Os recursos financeiros correrão por conta do Fundo Especial de Reaparelhamento e Modernização do Judiciário – FERMOJU, tendo como Fonte dos Recursos os Recursos Próprios, na seguinte dotação orçamentária:

**04200001.02.061.102.20181.22.33903900.15.2.00**
**04200001.02.061.102.20181.22.44905200.15.2.00**
**04200001.02.061.102.80037.22.33903900.15.2.00**
**04200001.02.061.102.80037.22.44905200.15.2.00**

## 17 DA RESCISÃO

17.1 O instrumento contratual firmado em decorrência da presente licitação poderá ser rescindido de conformidade com o disposto nos arts. 77 a 80 da Lei no 8.666/93.

17.2 Na hipótese de ocorrer a rescisão administrativa prevista no art. 79, inciso I, da Lei no 8.666/93, ao Contratante são assegurados os direitos previstos no art. 80, incisos I a IV, §§ 1o a 4o, da Lei citada.

## 18 DO CANCELAMENTO DO REGISTRO DE PREÇOS

18.1 A Ata de Registro de Preços poderá ser cancelada de pleno direito:

18.1.1 Pela autoridade competente do Órgão Gestor do Registro de Preços, mediante comunicação da unidade requisitante, quando:

18.1.1.1 o detentor não cumprir as obrigações dele constantes;

18.1.1.2 o detentor não assinar o contrato no prazo estabelecido e a unidade requisitante não aceitar sua justificativa;

18.1.1.3 o detentor der causa à rescisão administrativa da contratação decorrente deste instrumento de registro de preços, em alguma das hipóteses previstas no art. 78, inciso I a XII, ou XVII, da Lei Federal n.º 8.666/93, com as respectivas alterações posteriores;

18.1.1.4 em qualquer das hipóteses de inexecução total ou parcial da contratação decorrente deste instrumento de registro;

18.1.1.5 os preços registrados se apresentarem superiores aos praticados no mercado e o detentor não aceitar reduzir o preço registrado;

18.1.1.6 por razões de interesse público devidamente demonstradas e justificadas pela Administração.

18.1.2 Pelo detentor, quando, mediante solicitação por escrito, comprovar estar impossibilitado de cumprir as exigências nele contidas ou quando ocorrer alguma das hipóteses contidas no art. 78, incisos XIV e XVI da Lei Federal n.º 8.666/93, com as respectivas alterações posteriores.

18.1.2.1 A solicitação do detentor para cancelamento dos preços registrados deverá ser dirigida ao Órgão Gestor do Registro de Preços (Departamento de Informática - DEPIN/TJCE), facultada a esta, a aplicação das penalidades previstas, caso não aceitas as razões do pedido.

18.2 Ocorrendo o cancelamento do registro de preços pela Administração, o fornecedor detentor será comunicado por correspondência com aviso de recebimento, devendo este ser anexado ao processo que tiver dado origem ao registro de preços.

18.2.1 No caso de ser ignorado, incerto ou inacessível o endereço do detentor, a comunicação será feita por publicação no Diário Oficial da Estado, por 02 (duas) vezes consecutivas, considerando-se cancelado o preço registrado a partir da última publicação.

## 19 DAS OBRIGAÇÕES DAS PARTES

### 19.1 DO CONTRATANTE

a) A responsabilidade de fornecer todas as informações necessárias e que estiverem disponíveis para o desenvolvimento dos serviços objeto do presente contrato;

b) Notificar por escrito a CONTRATADA, fixando-lhe prazo para corrigir defeitos ou irregularidades encontrados na execução dos fornecimentos;

c) Indicar um gestor para o contrato, que será responsável pelo acompanhamento e fiscalização da sua execução, procedendo ao registro das ocorrências e adotando as providências necessárias ao seu fiel cumprimento, tendo por parâmetro os resultados previstos no contrato;

d) Efetuar os pagamentos devidos à CONTRATADA nas condições estabelecidas neste contrato;

e) Notificar a CONTRATADA sobre qualquer irregularidade encontrada na execução dos fornecimentos.

f) Fiscalizar a realização dos serviços e dos fornecimentos, por meio de sua unidade competente, podendo, em decorrência, solicitar providências previstas à CONTRATADA, que atenderá ou justificará de imediato. O não atendimento sujeitará a CONTRATADA às penalidades previstas neste Contrato.

g) Aplicar as penalidades previstas, na hipótese de a CONTRATADA não cumprir o contrato, mantidas as situações normais de disponibilidade e volume dos fornecimentos, arcando a referida com quaisquer prejuízos que tal ato trouxer ao CONTRATANTE.

### 19.2 DA CONTRATADA

a) Oferecer os serviços de acordo com o especificado nos ANEXOS deste Edital;

b) A CONTRATADA responsabilizar-se-á pelos danos causados diretamente à Administração ou a terceiros, decorrentes da sua culpa ou dolo quando da execução do contrato, objeto desta licitação, não podendo ser arguido, para efeito de exclusão de sua responsabilidade, o fato de a Administração proceder a fiscalização ou acompanhamento de execução dos referidos fornecimentos;

c) A CONTRATADA responderá por todas as despesas e obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências relativas ao objeto contratual, respondendo, especificamente, pelo fiel cumprimento das Leis Trabalhistas e Legislação correlata, aplicáveis ao pessoal empregado para executar os serviços e fornecimentos contratados;

d) A CONTRATADA assumirá as responsabilidades de pagamentos de todos os impostos, taxas e quaisquer ônus de origem Federal, Estadual e Municipal, ou que vierem a ser criados, bem como quaisquer encargos Judiciais ou Extrajudiciais que lhes sejam imputáveis, inclusive com relação a terceiros, em decorrência de celebração do contrato e da execução dos fornecimentos previstos;

e) Na vigência do contrato, a CONTRATADA terá o prazo máximo de cinco dias úteis subsequente ao término dos fornecimentos e serviços prestados mensalmente, para comprovar junto ao CONTRATANTE, todos os pagamentos legais e obrigatórios efetuados, inerentes a execução do objeto contratual;

f) Confiar os serviços a profissionais idôneos e habilitados, utilizando-se do mais alto nível da técnica atual;

g) Responsabilizar-se tecnicamente pela direção e execução dos fornecimentos objeto deste contrato, na forma da legislação em vigor;

h) Respeitar rigorosamente a legislação em vigor, bem como relativa a execução do objeto licitado;

i) Respeitar as normas de segurança e medicina do trabalho, previstas na Consolidação das Leis do Trabalho e legislação pertinente;

j) Fornecer ao seu pessoal os equipamentos de higiene e segurança adequados ao tipo de trabalho, bem como identificar e caracterizar seus empregados visualmente por meio de uniformes;

k) Manter-se durante toda a duração do contrato em compatibilidade com as obrigações assumidas, e com todas as condições de habilitação e qualificação exigidas na Lei de Licitações.

## 20 DISPOSIÇÕES FINAIS

20.1 A presente licitação não importa necessariamente em contratação, podendo o TJCE, revogá-la, no todo ou em parte, por razões de interesse público derivadas de fato superveniente comprovado ou anulá-la por ilegalidade, de ofício ou por provocação mediante ato escrito e fundamentado disponibilizado para conhecimento dos participantes da licitação. O(A) Pregoeiro(a) poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas ou para sua abertura;

20.2 O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado, ou a inverdade das informações nele contidas, implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis;

20.3 Os proponentes intimados para prestar quaisquer esclarecimentos adicionais, deverão fazê-lo no prazo determinado pelo(a) Pregoeiro(a), sob pena de desclassificação/ inabilitação;

20.4 O desatendimento de exigências formais não essenciais não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta;

20.5 As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa e do princípio da igualdade entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação;

20.6 As decisões referentes a este processo licitatório poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento ou, ainda, mediante publicação no Diário da Justiça;

20.7 Os casos não previstos neste Edital serão decididos pelo(a) Pregoeiro(a), nos termos da Legislação pertinente;

20.8 A participação do proponente nesta licitação implica em aceitação de todos os termos deste Edital;

20.9 O foro designado para julgamento de quaisquer questões judiciais resultantes deste Edital será o de Fortaleza, Capital do Estado do Ceará, considerado aquele a que está vinculado o Pregoeiro.

20.10 O Pregoeiro atenderá aos interessados no horário de 08:00 às 12:00 e das 13:00 às 17:00 horas, horário de Brasília, de segunda a sexta-feira, exceto feriados, ou por meio dos telefones (85) 3216.2654/2714/2551.

20.11 A documentação apresentada para fins de habilitação do licitante vencedor, fará parte dos autos da licitação e não será devolvida ao proponente, ainda que se trate de originais.

Fortaleza, aos 20 de agosto de 2010.

**Georgeanne Lima Gomes Botelho**
**PRESIDENTE DA COMISSÃO PERMANENTE DE LICITAÇÃO**

## ANEXO A - MODELO DE FICHA DE CREDENCIAMENTO

**MODALIDADE**: PREGÃO PRESENCIAL Nº _____/_____ - TJCE

**OBJETO:** A presente licitação tem como objeto o ***Registro de preços para aquisição de solução de segurança de TIC(Tecnologia da Informação e Comunicação), visando a interligação das unidades do Poder Judiciário, incluindo equipamentos destinados à sede do Tribunal, Fórum Clóvis Beviláqua e 209 (duzentas e nove) unidades judiciárias, bem como serviços de gerenciamento, suporte, atualização, implantação e treinamento da solução.***

Por meio do presente, credenciamos o(a) Sr.(a) _____, portador(a) da cédula de identidade nº _____ e do CPF nº _____, a participar da licitação instaurada pelo Tribunal de Justiça do Estado do Ceará na modalidade de PREGÃO PRESENCIAL, sob o nº 04/2010, na qualidade de REPRESENTANTE LEGAL, outorgando-lhe plenos poderes para pronunciar-se em nome da empresa _____, CNPJ nº _____, bem como formular propostas e praticar os demais atos inerentes ao certame.

Local e data.

_____
Identificação e assinatura do (s) dirigente(s) da empresa
(firma reconhecida)

Nome da Empresa:_____

CNPJ:_____

ENDEREÇO COMPLETO: _____ Nº _____

BAIRRO:_____ CIDADE: _____ CEP: _____

FONE: _____ FAX: _____

ENDEREÇO ELETRÔNICO DA EMPRESA:_____

PESSOA P/ CONTATO:_____

**Obs.:**

1. Caso o contrato social ou o estatuto determinem que mais de uma pessoa deva assinar o credenciamento, a falta de qualquer uma delas invalida o documento para os fins deste procedimento licitatório.

**2. Este credenciamento deverá vir acompanhado, obrigatoriamente, do ato de investidura do outorgante como dirigente da empresa.**

## ANEXO B - MODELO DE DECLARAÇÃO DA HABILITAÇÃO

(colocar em papel timbrado da empresa)

**Pregão Presencial n.º _____/____ -TJCE**

## DECLARAÇÃO

(nome da empresa) _____CNPJ nº _____ sediada _____. (Endereço completo) **declara**, sob as penas da Lei, que atende todos os requisitos de habilitação exigidos no Edital.

Fortaleza, ___de_____ de 2010.

Assinatura,
nome e número da identidade do declarante

## ANEXO C

## TERMO DE REFERÊNCIA

### 1 OBJETIVOS

Contratação de solução para interligação das Unidades do Poder Judiciário do Estado do Ceará utilizando VPNs (Virtual Private Networks), contemplando:

1.1 Contratação de solução para interligação das Unidades do Poder Judiciário do Estado do Ceará utilizando VPNs (Virtual Private Networks), contemplando:
- 1.1.1 Tribunal de Justiça, conforme tipos e especificações técnicas constantes no CÓDIGO 1;
- 1.1.2 Fórum Clóvis Beviláqua, conforme tipos e especificações técnicas constantes no CÓDIGO 2;
- 1.1.3 Unidades do Tribunal de Justiça, conforme tipos e especificações técnicas constantes no CÓDIGO 3;
- 1.1.4 Todos os equipamentos da solução de Firewall/VPN fornecidos devem ser de um mesmo fabricante.

1.2 Fornecimento de solução de IPS, conforme especificações técnicas constantes no CÓDIGO 4;

1.3 Fornecimento de solução de Console de gerenciamento centralizado da solução de Firewall conforme especificações técnicas constantes no CÓDIGO 5;

1.4 Fornecimento de solução de Console de gerenciamento centralizado da solução de IPS conforme especificações técnicas constantes no CÓDIGO 6;

1.5 Fornecimento de solução de Console Centralizada de Correlação de Eventos de Segurança, conforme especificações técnicas constantes no CÓDIGO 7;

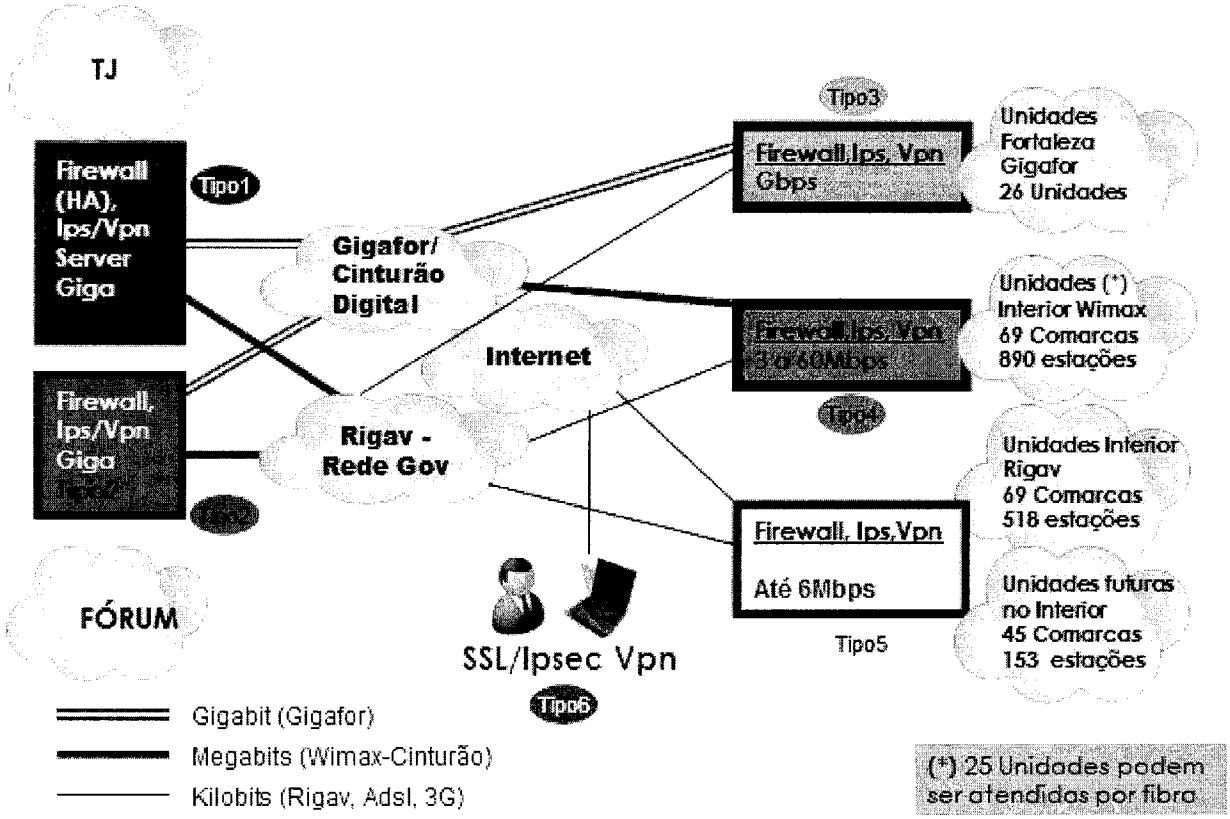
1.6 Serviços de operação gerenciada da solução, conforme especificações técnicas constantes no CÓDIGO 8;

Todas as unidades interligadas à rede deverão ser providas com equipamentos Firewall, sendo que na Sede do Tribunal de Justiça e no Fórum Clóvis Beviláqua serão instalados também equipamentos IPS (Intrusion Prevention System), Console de Gerência, sendo que o Correlacionador de Eventos será instalado somente na sede do TJCE. A empresa vencedora deverá prestar serviços de Gerenciamento e suporte para a solução.

### 2 DESCRIÇÃO GERAL DOS SERVIÇOS

2.1 Contratação de Empresa para Prestação de Serviços de Implantação e Gerenciamento da solução de segurança contratada.

2.2 O contrato deverá obedecer os seguintes prazos:
- 2.2.1 Garantia e suporte da solução de hardware e software: 36 (trinta e seis) meses;
- 2.2.2 Serviços de operação assistida da solução (código 08) : 12 (doze) meses;
- 2.2.3 Os serviços compreendem a instalação e gerenciamento 24x7x365 dos serviços de Firewall, Intrusion Prevention System (IPS) e VPN (Virtual Private Network) nas Unidades do Tribunal de Justiça;
- 2.2.4 Conforme apresentado na figura a seguir há 5 tipos de unidades para atendimento: Tipo 1 (Sede do TJ), Tipo 2 (Fórum), Tipo 3 (Rede atendida por fibra-Gigafor), Tipo 4 (Unidades Interior atendidas por Wimax ou fibra) e Tipo 5 (Unidades Interior atendidas pela Rede Governo-Rigav). Temos também o tipo 6 para representar as conexões de usuários de VPN remotos do TJ.




- **Visão Geral dos Serviços**

## 3 ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS E SERVIÇOS

### 3.1 CÓDIGO 01: Solução de Firewall/VPN para a Sede do Tribunal de Justiça

3.1.1 O conjunto da solução é composto por equipamentos de segurança de rede (appliance) com funcionalidades de Firewall/VPN.

3.1.2 A CONTRATADA deverá disponibilizar 02 (dois) equipamentos, configurados em alta disponibilidade e tolerância a falhas (ativo/ativo), de tal forma que o Firewall secundário assuma as funções do primário, mantendo o estado de todas as sessões ativas. O "failover" deve ser transparente para os usuários e aplicações;

3.1.3 Possuir LEDs indicativos do estado de funcionamento do equipamento;

3.1.4 O equipamento deve estar licenciado para um número ilimitado de estações;

3.1.5 Deve ser disponibilizado em um hardware com sistema operacional específico para o equipamento (appliance);

3.1.6 Não serão aceitas soluções baseadas em hardware de servidor de uso geral e em sistema operacional de uso geral, não customizado pelo fabricante do hardware para uso em Firewall;

3.1.7 Deve possuir tanto o software quanto o hardware do Firewall manufaturados, testados e suportados por um único fabricante;

3.1.8 Não serão aceitas soluções baseadas em sistema operacional de uso geral;

3.1.9 O hardware fornecido deverá possuir função exclusiva de Firewall/VPN. Appliances multifuncionais poderão ser ofertados, desde que tenham somente a funcionalidade de Firewall/VPN ativada, garantindo que a capacidade de processamento será toda dedicada a esta funcionalidade.

3.1.10 Possuir capacidade de inspecionar tráfego HTTP e FTP em portas diferentes das portas padrão;

3.1.11 A solução deve ser escalável, suportando a criação de um cluster com pelo menos 04 (quatro) equipamentos, possibilitando balanceamento de carga e redundância entre eles;

3.1.12 Hardware dedicado para funções de segurança de rede, com as

funcionalidades "Firewall Statefull Inspection", Gateway VPN IPSec, Gateway VPN Web/SSL; composto de hardware, software, firmware e acessórios necessários à sua instalação, configuração e operação completas;

3.1.13 Permitir integração nativa com Microsoft Active Directory e LDAP;

3.1.14 Permitir autenticação por meio de Radius;

3.1.15 Deve possibilitar a configuração de Firewall no modo transparente – Bridge Layer 2;

3.1.16 Deve implementer Network Address Translation (NAT) e Port Address Translation (PAT);

O dispositivo deve ser fisicamente independente, com gabinete e fonte de alimentação próprios, que possa implementar as funções descritas acima;

3.1.17 Deve possuir console de gerenciamento gráfica (GUI) centralizada e integrada para configuração das políticas de segurança corporativa, como também para administração do Firewall/VPN e gravação de registros de ocorrências (logs);

3.1.18 Possui suporte a listas de controle de acesso (ACL) IPV6 ou regras de controle acesso IPv6;

3.1.19 Deve suportar a configuração de QoS, alocação de banda e roteamento dinâmico OSPF;

3.1.20 A console de gerência deve ser capaz de suportar o gerenciamento de todos os Firewalls fornecidos, simultaneamente. Suas características estão descritas no CÓDIGO 5;

3.1.21 Deve ser fornecida solução de correlação de eventos de Segurança que suporte eventos gerados pelos sistemas de Firewall/VPN e IPS fornecidos. Suas características estão descritas no CÓDIGO 7.

3.1.22 Cada equipamento deve possuir 1 (hum) Gbps de throughput de Firewall;

3.1.23 Cada equipamento deve possuir 400 Mbps de throughput de VPN.

3.1.24 Cada equipamento deve possuir a capacidade de processar 650.000 sessões concorrentes de Firewall;

3.1.25 Cada equipamento deve possuir a capacidade de processar 5.000 túneis de VPN IPSec;

3.1.26 Cada equipamento deve possuir pelo menos 08 (oito) portas RJ-45, para cabos UTP-5 enhanced, 10/100/1000 BaseTX, full duplex, ethernet, auto-sense;

3.1.27 Cada equipamento deve possuir a capacidade de processar VPN Site-to-Site e Client-to-Site;

3.1.28 A CONTRATADA deverá disponibilizar clientes de VPN IPSec com suporte para os sistemas operacionais Windows XP e Vista;

3.1.29 Deverá ser fornecido software cliente de VPN com as seguintes funcionalidades:

3.1.29.1 Deve permitir a criação de políticas de VPN distintas para cada perfil de usuário, sendo que para cada uma destas políticas poderão ser definidos regras de acesso (ACLs), horário, autenticação, criptografia, endereçamento IP e rotas criptografadas;

3.1.29.2 A quantidade de clientes a ser atendida deverá ser no mínimo igual a 1.000 (hum mil);

3.1.29.3 Os usuários da VPN deverão ser autenticados e autorizados diretamente no LDAP, onde cada política de VPN definida no firewall terá um grupo no LDAP;

3.1.29.4 Permitir VPN com controle granular de acesso aos recursos da rede corporativa, podendo-se definir que servidores, recursos, serviços e portas podem ser acessados por conexão VPN.

3.1.29.5 Implementar VPN com Gerenciamento centralizado e distribuição automática de políticas por conexão VPN por meio da console de gerência descrita no CÓDIGO 5.

3.1.29.6 Permitir autenticação forte de usuário de VPN, por meio da utilização de tokens e certificados digitais emitidos pela CA do Tribunal de Justiça.

3.1.29.7 Permitir autenticação de computadores remotos na VPN por meio de

certificados digitais emitidos pela CA do Tribunal de Justiça.

3.1.29.8 Permitir autenticação forte de conexão VPN LAN-TO-LAN, por meio de certificados digitais emitidos pela CA do Tribunal de Justiça.

3.1.29.9 Permitir atualização automática do cliente de VPN.

3.1.29.10 Ativação de firewall pessoal no computador do usuário para conexão VPN, permitindo que se bloqueie o acesso de qualquer elemento da rede remota aos recursos da rede interna do Tribunal de Justiça.

3.1.29.11 O cliente de VPN deve suportar NAC na VPN, possibilitando a checagem da conformidade do computador que está tentando se conectar a rede;

3.1.29.12 Possuir suporte a Virtual LANs (VLANs) conforme padrão IEEE 802.1Q;

3.1.29.13 Possuir console de administração remota por meio de canal protegido, onde as informações trafeguem de forma criptografada;

3.1.29.14 Recursos de QoS:

3.1.29.14.1 A solução deve implementar Priority Queue para tráfego de Voz e Vídeo;

3.1.29.14.2 A solução deve implementar Rate Limiting para qualquer tipo de tráfego TCP/UDP;

3.1.29.14.3 Deverá possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas;

3.1.29.14.4 A fonte alimentação deverá funcionar com tensão elétrica nominal de 110V~220V AC, 50~60Hz, de modo automático;

3.1.29.14.5 A solução deverá acompanhar documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

3.1.30 A solução deverá ser disponibilizada com todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos lógicos, cabos de interface RS-232 e cabos de energia elétrica.

3.1.31 Os equipamentos deverão processar protocolos VoIP, incluindo SIP e H.323;

3.1.32 Possuir suporte ao protocolo de gerenciamento SNMP;

### 3.2 CÓDIGO 02: Solução de Firewall/VPN para o Fórum

3.2.1 O conjunto da solução é composto por equipamentos de segurança de rede (appliance) com funcionalidades de Firewall/VPN.

3.2.2 A CONTRATADA deverá disponibilizar 01 (hum) equipamento;

3.2.3 Possuir LEDs indicativos do estado de funcionamento do equipamento;

3.2.4 O equipamento deve estar licenciado para um número ilimitado de estações;

3.2.5 Deve ser disponibilizado em um hardware com sistema operacional específico para o equipamento (appliance);

3.2.6 Não serão aceitas soluções baseadas em hardware de servidor de uso geral e em sistema operacional de uso geral, não customizado pelo fabricante do hardware para uso em Firewall;

3.2.7 Deve possuir tanto o software quanto o hardware do Firewall manufaturados, testados e suportados por um único fabricante;

3.2.8 Não serão aceitas soluções baseadas em sistema operacional de uso geral;

3.2.9 O hardware fornecido deverá possuir função exclusiva de Firewall/VPN. Appliances multifuncionais poderão ser ofertados, desde que tenham somente a funcionalidade de Firewall/VPN ativada, garantindo que a capacidade de processamento será toda dedicada a esta funcionalidade.

3.2.10 Possuir capacidade de inspecionar tráfego HTTP e FTP em portas diferentes das portas padrão;

3.2.11 A solução deve ser escalável, suportando a criação de um cluster com pelo menos 04 (quatro) equipamentos, possibilitando balanceamento de carga e redundância entre eles;

3.2.12 Hardware dedicado para funções de segurança de rede, com as

funcionalidades "Firewall Statefull Inspection", Gateway VPN IPSec, Gateway VPN Web/SSL; composto de hardware, software, firmware e acessórios necessários à sua instalação, configuração e operação completas;

3.2.13 Permitir integração nativa com Microsoft Active Directory e LDAP;

3.2.14 Permitir autenticação por meio de Radius;

3.2.15 Deve possibilitar a configuração de Firewall no modo transparente – Bridge Layer 2;

3.2.16 Deve implementer Network Address Translation (NAT) e Port Address Translation (PAT);

3.2.17 O dispositivo deve ser fisicamente independente, com gabinete e fonte de alimentação próprios, que possa implementar as funções descritas acima;

3.2.18 Deve possuir console de gerenciamento gráfica (GUI) centralizada e integrada para configuração das políticas de segurança corporativa, como também para administração do Firewall/VPN e gravação de registros de ocorrências (logs);

3.2.19 Possui suporte a listas de controle de acesso (ACL) Ipv6 ou regras de controle acesso IPv6;

3.2.20 Possuir suporte ao protocolo de gerenciamento SNMP;

3.2.21 Deve suportar a configuração de QoS, alocação de banda e roteamento dinâmico OSPF;

3.2.22 A console de gerência deve ser capaz de suportar o gerenciamento de todos os Firewalls fornecidos, simultaneamente. Suas características estão descritas no CÓDIGO 5;

3.2.23 Deve ser fornecida solução de correlação de eventos de Segurança que suporte eventos gerados pelos sistemas de Firewall/VPN e IPS fornecidos. Suas características estão descritas no CÓDIGO 7.

3.2.24 O equipamento deve possuir 1 (hum) Gbps de throughput de Firewall;

3.2.25 O equipamento deve possuir 400 Mbps de throughput de VPN.

3.2.26 O equipamento deve possuir a capacidade de processar 650.000 sessões concorrentes de Firewall;

3.2.27 O equipamento deve possuir a capacidade de processar 5.000 túneis de VPN IPSec;

3.2.28 O equipamento deve possuir pelo menos 08 (oito) portas RJ-45, para cabos UTP-5 enhanced, 10/100/1000 BaseTX, full duplex, ethernet, auto-sense;

3.2.29 O equipamento deve possuir a capacidade de processar VPN Site-to-Site e Client-to-Site;

3.2.30 A CONTRATADA deverá disponibilizar clientes de VPN IPSec com suporte para os sistemas operacionais Windows XP e Vista;

3.2.31 Deverá ser fornecido software cliente de VPN com as seguintes funcionalidades:

3.2.31.1 O cliente de VPN deve suportar NAC na VPN, possibilitando a checagem da conformidade do computador que está tentando se conectar a rede;

3.2.31.2 Deve permitir a criação de políticas de VPN distintas para cada perfil de usuário, sendo que para cada uma destas políticas poderão ser definidos regras de acesso (ACLs), horário, autenticação, criptografia, endereçamento IP e rotas criptografadas;

3.2.31.3 A quantidade de clientes a ser atendida deverá ser no mínimo igual a 1.000 (hum mil);

3.2.31.4 Os usuários da VPN deverão ser autenticados e autorizados diretamente no LDAP, onde cada política de VPN definida no firewall terá um grupo no LDAP;

3.2.31.5 Permitir VPN com controle granular de acesso aos recursos da rede corporativa, podendo-se definir que servidores, recursos, serviços e portas podem ser acessados por conexão VPN.

3.2.31.6 Implementar VPN com Gerenciamento centralizado e distribuição automática de políticas por conexão VPN por meio da console de gerência

descrita no CÓDIGO 5.

3.2.31.7 Permitir autenticação forte de usuário de VPN, por meio da utilização de tokens e certificados digitais emitidos pela CA do Tribunal de Justiça.

3.2.31.8 Permitir autenticação de computadores remotos na VPN por meio de certificados digitais emitidos pela CA do Tribunal de Justiça.

3.2.31.9 Permitir autenticação forte de conexão VPN LAN-TO-LAN, por meio de certificados digitais emitidos pela CA do Tribunal de Justiça.

3.2.31.10 Permitir atualização automática do cliente de VPN.

3.2.31.11 Ativação de firewall pessoal no computador do usuário para conexão VPN, permitindo que se bloqueie o acesso de qualquer elemento da rede remota aos recursos da rede interna do Tribunal de Justiça.

3.2.31.12 Possuir suporte a Virtual LANs (VLANs) conforme padrão IEEE 802.1Q;

3.2.31.13 Possuir console de administração remota por meio de canal protegido, onde as informações trafeguem de forma criptografada;

3.2.31.14 Recursos de QoS:

3.2.31.15 A solução deve implementar Priority Queue para tráfego de Voz e Vídeo;

3.2.31.16 A solução deve implementar Rate Limiting para qualquer tipo de tráfego TCP/UDP;

3.2.32 Os equipamentos deverão processar protocolos VoIP, incluindo SIP e H.323;

3.2.33 Deverá possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas;

3.2.34 A fonte alimentação deverá funcionar com tensão elétrica nominal de 110V~220V AC, 50~60Hz, de modo automático.

3.2.35 A solução deverá acompanhar documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

3.2.36 A solução deverá ser disponibilizada com todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos lógicos, cabos de interface RS-232 e cabos de energia elétrica.

3.3 **CÓDIGO 03: Solução de Firewall/VPN para as Unidades do Tribunal de Justiça**

3.3.1 O conjunto da solução é composto por equipamentos de segurança de rede (appliance) com funcionalidades de Firewall/VPN.

3.3.2 A CONTRATADA deverá disponibilizar 209 (duzentos e nove) equipamentos;

3.3.3 Possuir LEDs indicativos do estado de funcionamento do equipamento;

3.3.4 O equipamento deve estar licenciado de acordo com a estratificação abaixo:

3.3.4.1 Licenciamento até 50 usuários/estações de trabalho;

3.3.4.2 Licenciamento até 150 usuários/estações de trabalho;

3.3.4.3 Licenciamento para um número ilimitado de usuários;

3.3.4.4 O valor do licenciamento deve ser informado conforme exigido no ANEXO D – Planilha de Composição de Custos;

3.3.5 Deve ser disponibilizado em um hardware com sistema operacional específico para o equipamento (appliance);

3.3.6 Não serão aceitas soluções baseadas em hardware de servidor de uso geral e em sistema operacional de uso geral, não customizado pelo fabricante do hardware para uso em Firewall;

3.3.7 Deve possuir tanto o software quanto o hardware do Firewall manufaturados, testados e suportados por um único fabricante;

3.3.8 O hardware fornecido deverá possuir função exclusiva de Firewall/VPN. Appliances multifuncionais poderão ser ofertados, desde que tenham somente a funcionalidade de Firewall/VPN ativada, garantindo que a capacidade de processamento será toda dedicada a esta funcionalidade.

3.3.9 Possuir capacidade de inspecionar tráfego HTTP e FTP em portas diferentes das portas padrão;

3.3.10 Deve possuir o software pré-instalado e disponibilizado em memória flash, dispensando assim a necessidade de discos rígidos na solução;

3.3.11 Hardware dedicado para funções de segurança de rede, com as funcionalidades "Firewall Statefull Inspection", Gateway VPN IPSec; composto de hardware, software, firmware e acessórios necessários à sua instalação, configuração e operação completas;

3.3.12 Permitir integração nativa com Microsoft Active Directory, Microsoft Windows Domains e LDAP;

3.3.13 Permitir autenticação por meio de Radius;

3.3.14 Deve implementer Network Address Translation (NAT) e Port Address Translation (PAT);

3.3.15 O dispositivo deve ser fisicamente independente, com gabinete e fonte de alimentação próprios, que possa implementar as funções escritas acima;

3.3.16 Deve possuir console de gerenciamento gráfica (GUI) centralizada e integrada para configuração das políticas de segurança corporativa, como também para administração do Firewall/VPN e gravação de registros de ocorrências (logs);

3.3.17 Possui suporte a listas de controle de acesso (ACL) Ipv6 ou regras de controle acesso IPv6;

3.3.18 Possuir suporte ao protocolo de gerenciamento SNMP;

3.3.19 Deve suportar a configuração de QoS, alocação de banda e roteamento dinâmico OSPF;

3.3.20 A console de gerência deve ser capaz de suportar o gerenciamento de todos os Firewalls fornecidos simultaneamente. Suas características estão descritas no CÓDIGO 5;

3.3.21 Deve ser fornecida solução de correlação de eventos de Segurança que suporte eventos gerados pelos sistemas de Firewall/VPN fornecidos. Suas características estão descritas no CÓDIGO 7.

3.3.22 O equipamento deve possuir 130 Mbps de throughput de Firewall;

3.3.23 O equipamento deve possuir 90 Mbps de throughput de VPN.

3.3.24 O equipamento deve possuir a capacidade de processar 10.000 sessões concorrentes de Firewall;

3.3.25 O equipamento deve possuir a capacidade de processar 10 túneis de VPN IPSec;

3.3.26 O equipamento deve possuir pelo menos 05 (cinco) portas RJ-45, para cabos UTP-5 enhanced, 10/100BaseTX, full duplex, ethernet, auto-sense;

3.3.27 O equipamento deve possuir a capacidade de processar VPN Site-to-Site e Client-to-Site;

3.3.28 A CONTRATADA deverá suportar clientes de VPN IPSec com suporte para os sistemas operacionais Windows XP e Vista;

3.3.29 Possuir suporte a Virtual LANs (VLANs) conforme padrão IEEE 802.1Q;

3.3.30 Possuir console de administração remota por meio de canal protegido, onde as informações trafeguem de forma criptografada;

3.3.31 Recursos de QoS:

3.3.31.1 A solução deve implementar Priority Queue para tráfego de Voz e Vídeo;

3.3.31.2 A solução deve implementar Rate Limiting para qualquer tipo de tráfego TCP/UDP;

3.3.32 Os equipamentos deverão processar protocolos VoIP, incluindo SIP e H.323;

3.3.33 A fonte alimentação deverá funcionar com tensão elétrica nominal de 110V~220V AC, 50~60Hz, de modo automático.

3.3.34 A solução deverá acompanhar documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

3.3.35 A solução deverá ser disponibilizada com todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos lógicos, cabos de interface RS-232 e cabos de energia elétrica.

3.3.36 Deve possibilitar a configuração de Firewall no modo transparente – Bridge Layer 2;

## 3.4 CÓDIGO 04: Solução de IPS

3.4.1 O conjunto da solução é composto por equipamentos de segurança de rede (appliance) com funcionalidades de IPS.

3.4.2 A CONTRATADA deverá disponibilizar 02 (dois) equipamentos de IPS em conformidade com as exigências expostas a seguir.

3.4.3 A solução oferecida deve ser contemplada em tecnologia "Appliance";

3.4.4 Deve permitir montagem em rack de 19 polegadas;

3.4.5 O hardware fornecido deverá possuir função exclusiva de IPS. Appliances multifuncionais poderão ser ofertados, desde que tenham somente a funcionalidade de IPS ativada, garantindo que a capacidade de processamento será toda dedicada a esta funcionalidade.

3.4.6 Deverá possuir funcionalidade de "software bypass" , ou seja, em caso de falha em algum processo do software do IPS o mesmo deverá desabilitar o monitoramento.

3.4.7 Deverá implementar funcionalidade de "hardware bypass" de forma automática, ou seja, em caso de qualquer falha em hardware (falha de hardware, falha de energia, desligamento do IPS etc.) o IPS deverá permitir a passagem do tráfego sem perda de conectividade. Essa funcionalidade deverá ser interna ao equipamento. Caso o equipamento não implemente esse funcionalidade internamente alternativamente será aceita utilização de um appliance secundário, com as mesmas características do equipamento fornecido, desde que não interrompa o fluxo dos dados. O appliance secundário deverá ser fornecido, caso necessário, sem quaisquer custos adicionais ao TJCE e obedecer as mesmas condições de garantia do equipamento ofertado;

3.4.8 O equipamento deve possuir no mínimo 1.5 Gbps de throughput de IPS. Para fins de comprovação, no caso de o fabricante informar mais de um valor de throughput de IPS para o seu equipamento (dependendo do tipo de tráfego), será considerada a média aritmética entre o maior e o menor valor informado;

3.4.9 O equipamento deve possuir fonte de alimentação redundante;

3.4.10 O equipamento deve possuir pelo menos 08 (oito) portas RJ-45, para cabos UTP-5 enhanced, 10/100/1000BaseTX, com a capacidade de monitorar segmentos de rede ethernet em 10, 100 e 1000 Mbps;

3.4.11 O equipamento deve possuir no mínimo 01 (uma) interface 10/100Base-TX para gerenciamento e controle.

3.4.12 Deve possuir alimentação elétrica AC com comutação automática de 110 e 220V;

3.4.13 O sistema de detecção de intrusão deve ser composto por dois elementos: sensor ("probe") e console de gerenciamento . A probe deverá ser responsável por monitorizar a rede a que está conectada, analisando tanto o cabeçalho(header) como a área de dados (payload) de cada pacote que trafega pela rede citada, de modo a verificar se os referidos pacotes constituem tráfego autorizado.

3.4.14 A console de gerenciamento deverá permitir a configuração gráfica dos sensores ("probes") e receber os alertas e notificações de ataques de todos os sensores que monitoram a rede.

3.4.15 Toda a comunicação entre o sensor e a console de gerenciamento deve ser criptografada.

3.4.16 Funcionalidade para detectar ataques em tempo real.

3.4.17 O sensor deverá ser capaz de enviar reset TCP por uma interface de monitoramento ou por meio de interface dedicada.

3.4.18 Deve permitir operação em modo promíscuo (IDS) e no modo "in-line" (IPS),

descartando pacotes identificados como associados a ataques.

3.4.19 Deve ser possível especificar quais interfaces ou assinaturas operam no modo IDS e quais operam no modo IPS. O IPS deverá ser capaz de operar nos dois modos simultaneamente.

3.4.20 Capacidade de detecção de intrusos e ataques no segmento de rede que está monitorando e analisando;

3.4.21 Deve suportar a análise simultânea de tráfego associado à pelo menos 250 VLANs IEEE 802.1q.

3.4.22 Deve ser capaz de operar no modo "in-line" monitorando múltiplos segmentos (VLAN) de rede utilizando uma única interface.

3.4.23 Deve ser capaz de monitorizar o tráfego de redes TCP/IP, incluindo: redes locais, conexões Internet e conexões discadas.

3.4.24 Deve analisar cada um dos pacotes que trafegam pela rede a que está conectado e também a relação de tais pacotes com os adjacentes a ele no fluxo de dados da rede (análise de contexto). Imediatamente após a identificação de uma eventual violação da política de segurança o sensor deve enviar um alarme para o software de controle.

3.4.25 Deverá ter uma base de assinaturas com descrição da utilização de cada uma delas e tipos de ataques detectados. Deverá ser possível a atualização gratuita de assinaturas em caso de detecção de novas vulnerabilidades durante a vigência do contrato de suporte.

3.4.26 Deve suportar a modificação de assinaturas, isto é, permitir a edição de assinaturas existentes na base de dados, ajustando-se ao perfil de tráfego de rede;

3.4.27 Deve suportar a criação de assinaturas, isto é, permitir que se possam criar novas assinaturas e anexá-las à base de dados existente, adaptando-se as reais necessidades de tráfego de rede (na criação das novas assinaturas deve ser permitida a utilização de parâmetros de nível 2 a nível 7 do modelo OSI);

3.4.28 Deve ser possível criar assinaturas do tipo "string-match" e associá-las a qualquer porta TCP para verificação da ocorrência de conjunto de caracteres definidos pelo administrador de política de segurança no conteúdo dos pacotes IP que trafegam pela rede.

3.4.29 O software de controle deve ser capaz de enviar alarmes para um sistema de pager ou via e-mail para notificar a violação de uma dada regra de segurança.

3.4.30 O sistema deve registrar informações tais como origem, destino, horário e tipo dos ataques ocorridos.

3.4.31 Deve implementar "Protocol Anomaly Detection" como método de análise de tráfego.

3.4.32 Deverá implementar funcionalidade de detecção de anomalias protegendo dessa forma contra ataques do dia zero. O sensor deverá detectar mudanças no comportamento padrão da rede e bloquear ataques de Worms e ataques sem a necessidade de uma assinatura para o mesmo.

3.4.33 Deverá ser possível habilitar a análise passiva do tráfego da rede durante um período agendado a fim de aprendizado do comportamento padrão da rede. Após esse período deverá ser possível habilitar a proteção baseada no aprendizado, permitindo assim a detecção automática do Tráfego anômalo na rede.

3.4.34 Deverá ser possível especificar uma ação baseada no detecção da anomalia (Geração de Alarme, Logs dos pacotes, ou bloqueio do trafego inline);

3.4.35 Deverá verificar conformidades constantes nas RFCs (análise de "RFC compliance");

3.4.36 Deve suportar análise "stateful" de pacotes para garantir maior precisão de detecção ("Stateful Pattern Matching");

3.4.37 Deve suportar detecção de anomalias de tráfego da Rede (anomalias associadas a definições estatísticas de tráfego);

3.4.38 Deve detectar ataques associados a protocolos que não estejam usando as portas canônicas de serviço (portas padrão reservadas para os protocolos de aplicação);

3.4.39 Deve promover reordenação e remontagem de fragmentos IP antes de efetuar análise.

3.4.40 Deve possuir estrutura de "normalização" de tráfego para que possam combater as técnicas de evasão;

3.4.41 Deve ser possível identificar o sistema operacional associado a um determinado endereço IP permitindo dessa forma analise do risco associado a um determinado ataque.

3.4.42 Além da geração de alarmes em caso de detecção de tentativa de ataque, o sistema deve ser capaz de reagir em tempo real a uma tal tentativa. As reações devem ser configuradas por assinatura.

3.4.43 Quando da operação em modo "in-line"(IPS) devem ser suportados no mínimo os seguintes tipos de reação (configuráveis por assinatura de ataque): geração de alerta, gerar trap SNMP, fazer "logging"dos pacotes gerados pelo sistema "vítima", fazer "logging" dos pacotes gerados pelo sistema que está efetuando o ataque, promover "reset" da conexão TCP, bloquear o pedido de conexão, bloquear o endereço que está gerando o ataque de conexão, negar pacotes associados ao ataque "in-line".

3.4.44 O sistema suporta "logging" de sessão via IP ("IP session logging"). Os logs devem ser compatíveis com formato "TCPDump".

3.4.45 Deve possuir opção de gravação de sessões completas para servir como subsídio para análise forense (IP Session Logging). Estes dados devem ficar armazenados em arquivos no sensor e ser visualizáveis por meio da console de gerência. Estes arquivos devem ser protegidos por controle de acesso.

3.4.46 Capacidade de gerar relatórios customizados, por sensor, por horário, por evento, por endereço, por porta.

3.4.47 A console de gerência deve ser capaz de suportar o gerenciamento todos IPSs fornecidos simultaneamente.

3.4.48 O sistema deve registrar informações tais como origem, destino, horário e tipo dos ataques ocorridos.

3.4.49 Deve ser fornecida solução de correlação de eventos de Segurança que suporte eventos gerados pelos sistemas de detecção/prevenção de intrusão fornecidos. Suas características estão descritas no CÓDIGO 7.

## 3.5 CÓDIGO 05: Console de Gerenciamento Centralizado da Solução de Firewall

3.5.1 A CONTRATADA deve fornecer uma console de gerenciamento centralizado das soluções de Firewall/VPN.

3.5.2 A CONTRATADA deverá fornecer toda plataforma de hardware e software devidamente licenciada para solução de gerenciamento as soluções de Firewall/VPN.

3.5.3 O Software da solução de gerenciamento de segurança deve ser do mesmo fabricante dos equipamentos Firewall/VPN.

3.5.4 A solução de gerenciamento de segurança deve ser baseada em técnicas de aplicação e gerenciamento de políticas de forma centralizada, as quais podem ser organizadas de forma hierárquica e distribuídas para grupos de dispositivos de segurança ou para todos os dispositivos de segurança já existentes da rede ou não.

3.5.5 A solução deve implementar uma tabela única de políticas de segurança, a qual deverá ser utilizada para a distribuição das políticas por todo o ambiente administrado;

3.5.6 As políticas de segurança dever ser automaticamente adaptadas de acordo com o dispositivo para o qual ela está sendo enviada;

3.5.7 A solução deve implementar funcionalidade de agrupamento de políticas que façam referência a um objeto específico a ser analisado de forma a transformar esse grupo de políticas em uma única regra que desempenhará o mesmo papel na política de segurança proposta por um conjunto de regras;

3.5.8 A solução deve possuir ferramenta de análise das regras, permitindo que

sejam analisadas as regras que estão se sobrepondo ou entrando em conflito com outras regras já existentes;

3.5.9 A solução deve permitir a identificação e exclusão de regras que estão aplicadas nos dispositivos, mas não afetam o desempenho e/ou a segurança da rede;

3.5.10 A solução deve implementar a contabilidade das Listas de Controle de Acesso - ACLs - que foram atingidas ou entraram em conformidade com o tráfego que está passando pela rede;

3.5.11 A solução deve permitir a verificação de qual parte da rede, origem, destino, serviço ou wildcard, está sendo atingido por determinada regra;

3.5.12 A solução deve permitir a detecção de alteração e/ou tentativas de alteração nos dispositivos;

3.5.13 A solução deve permitir o gerenciamento de serviços de segurança integrados, entre os quais QoS em VPN, roteamento e Controle de Acesso a Rede;

3.5.14 A solução deve permitir o agrupamento de dispositivos, de acordo com a funcionalidade e/ou localização física dos mesmos, com a finalidade de gerenciar todos os dispositivos de uma só vez;

3.5.15 A solução deve permitir que um dado equipamento possa pertencer a mais de um grupo simultaneamente;

3.5.16 A solução deve permitir a reutilização de objetos a serem analisados e/ou monitorados em um dispositivo por outros dispositivos que vierem a fazer parte do ambiente, sem a necessidade da criação das mesmas políticas novamente;

3.5.17 A solução deve permitir o retorno às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas;

3.5.18 A solução deve permitir o gerenciamento operacional da rede monitorada, realizando funções de distribuição de softwares, relatório de inventário de dispositivos.

3.5.19 A solução deve ser capaz de testar a conectividade de equipamentos já foram ou estão sendo adicionados;

3.5.20 A solução deve permitir a configuração de servidores de syslog e NTP nos equipamentos suportados;

3.5.21 A solução deve suportar configuração de alta-disponibilidade dos equipamentos;

3.5.22 A solução deve oferecer a opção de se apresentar um mapa onde é possível indicar a localização dos equipamentos;

3.5.23 A solução deve ser capaz de descobrir configurações existentes de VPN site-to-site e acesso remoto;

3.5.24 A solução deve permitir as configurações de VPN nas seguintes modalidades: site-to-site, hub-and-spoke, full-mesh e extranet;

3.5.25 A solução deve permitir que as VPNs possam ser configuradas remotamente;

3.5.26 A solução deve permitir a configuração de dispositivos de VPN com suporte a failover automático e balanceamento de carga;

3.5.27 A solução deve suportar operar em modo de "workflow", quando é necessário uma aprovação para a distribuição de configurações;

3.5.28 A solução deve suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;

3.5.29 O acesso aos equipamentos devem ser também ser separados por perfil de usuário;

3.5.30 Serão aceitas soluções de gerenciamento de segurança integrada para os equipamentos de Firewall/VPN e IPS.

## 3.6 CÓDIGO 06: Console de Gerenciamento Centralizado da Solução de IPS

3.6.1 A CONTRATADA deve fornecer uma console de gerenciamento centralizado das soluções de IPS.

3.6.2 A CONTRATADA deverá fornecer toda plataforma de hardware e software

devidamente licenciada para solução de gerenciamento a das soluções de IPS.

3.6.3 O Software da solução de gerenciamento de segurança deve ser do mesmo fabricante dos equipamentos de IPS disponibilizados.

3.6.4 A solução de gerenciamento de segurança deve ser baseada em técnicas de aplicação e gerenciamento de políticas de forma centralizada, as quais podem ser organizadas de forma hierárquica e distribuídas para grupos de dispositivos de segurança ou para todos os dispositivos de segurança já existentes da rede ou não.

3.6.5 A solução deve implementar uma tabela única de políticas de segurança, a qual deverá ser utilizada para a distribuição das políticas por todo o ambiente administrado;

3.6.6 As políticas de segurança dever ser automaticamente adaptadas de acordo com o dispositivo para o qual ela está sendo enviada;

3.6.7 A solução deve implementar funcionalidade de agrupamento de políticas que façam referência a um objeto específico a ser analisado de forma a transformar esse grupo de políticas em uma única regra que desempenhará o mesmo papel na política de segurança proposta por um conjunto de regras;

3.6.8 A solução deve possuir ferramenta de análise das regras, permitindo que sejam analisadas as regras que estão se sobrepondo ou entrando em conflito com outras regras já existentes;

3.6.9 A solução deve permitir a identificação e exclusão de regras que estão aplicadas nos dispositivos, mas não afetam o desempenho e/ou a segurança da rede;

3.6.10 A solução deve implementar a contabilidade das Listas de Controle de Acesso - ACLs - que foram atingidas ou entraram em conformidade com o tráfego que está passando pela rede;

3.6.11 A solução deve permitir a verificação de qual parte da rede, origem, destino, serviço ou wildcard, está sendo atingido por determinada regra;

3.6.12 A solução deve permitir a detecção de alteração e/ou tentativas de alteração nos dispositivos;

3.6.13 A solução deve permitir o agrupamento de dispositivos, de acordo com a funcionalidade e/ou localização física dos mesmos, com a finalidade de gerenciar todos os dispositivos de uma só vez;

3.6.14 A solução deve permitir que um dado equipamento possa pertencer a mais de um grupo simultaneamente;

3.6.15 A solução deve permitir a reutilização de objetos a serem analisados e/ou monitorados em um dispositivo por outros dispositivos que vierem a fazer parte do ambiente, sem a necessidade da criação das mesmas políticas novamente;

3.6.16 A solução deve permitir o retorno às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas;

3.6.17 A solução deve permitir a configuração de servidores de syslog e NTP nos equipamentos suportados;

3.6.18 A solução deve suportar configuração de alta-disponibilidade dos equipamentos;

3.6.19 A solução deve oferecer a opção de se apresentar um mapa onde é possível indicar a localização dos equipamentos;

3.6.20 A solução deve suportar operar em modo de "workflow", quando é necessário uma aprovação para a distribuição de configurações;

3.6.21 A solução deve suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política;

3.6.22 O acesso aos equipamentos devem ser também ser separados por perfil de usuário;

### 3.7 CÓDIGO 07: Console Centralizada de Correlação de Eventos de Segurança

3.7.1 A CONTRATADA deve fornecer uma console centralizado de correlação de eventos de segurança, do mesmo fabricante das soluções de Firewall/VPN e IPS,

ou, se for de fabricante distinto, acompanhado de documentação do fabricante da solução de Correlação de Enventos informando haver compatibilidade nativa entre sua solução e solução de Firewall/VPN proposta (será aceito como comprovação somente documentação no formato especificado no item 9.2.1).

3.7.2 Todo o hardware e software necessário para execução da solução deverá ser fornecido.

3.7.3 Esta solução deve suportar o processamento de pelo menos 1.500 eventos por segundo (syslog, SNMP, SDEE, RDEP) e ser acessível por meio de interface gráfica de configuração e análise de eventos.

3.7.4 Deve ser possível traçar o caminho seguido pelos pacotes de ataque ao longo da rede gerenciada.

3.7.5 A solução de correlação de eventos deve ser capaz de processar informações de fluxos "Netflow" gerados pelos roteadores da Rede. Deve ser possível estabelecer a característica padrão de tráfego da rede por meio das informações Netflow coletadas e detectar automaticamente desvios em relação a estes valores padrão.

3.7.6 A solução deve correlacionar informações sobre os fluxos Netflow com eventos gerados pelos produtos de IPS de Rede (Network Intrusion Prevention System)

3.7.7 A solução deve ser capaz de tratar pelo 30.000 fluxos "Netflow" por segundo.

3.7.8 Permitir a administração gráfica de incidentes. Deve ser possível usar os conceitos de casos abertos, casos fechados e casos escalados para acompanhamento do progresso da resolução de um dado incidente de Segurança. Em cada caso gerado deve ser possível acrescentar informações tais como: comentários do administrador de Segurança sobre o andamento do caso e ações tomadas e relatórios sobre atividade da máquina atacada.

3.7.9 A solução deve ter recursos para agregar informações associadas a eventos gerados por um dado endereço IP e pelo correspondente endereço IP traduzido (via NAT), de modo a gerar uma análise unificada (inteligência para tratar NAT e resolver redundância de informação).

3.7.10 A solução deve ser capaz de correlacionar eventos associados a acessos às Redes locais que façam uso de autenticação/autorização IEEE 802.1x (coletando informações diretamente dos switches de rede e também da solução de controle de acesso).

3.7.11 A solução deve ser capaz de correlacionar informações relativas ao controle de admissão à Rede ("Network Admission Control"), efetuado por roteadores, switches e concentradores VPN. Deve ser possível detectar porque um dado usuário teve acesso negado no momento da validação de suas credenciais de "status" e gerar relatórios correspondentes.

3.7.12 A solução deve ter mecanismo interno para minimização de alarmes falsos ("false positives").

3.7.13 A solução deve permitir expandir os registros de um incidente de forma que possa ser visualizado cada evento que faz parte do incidente.

3.7.14 A solução deve permitir que, a partir de cada evento, seja possível investigar outros eventos que tenham a origem, destino, protocolo ou tipo de evento do evento atual.

3.7.15 Suporte a geração de relatórios (em tempo real e agendados) com filtragem por endereços IP de origem, endereços IP de destino, portas TCP/UDP, tipo de ataque, eventos gerados por um dado equipamento, etc. Deve ser possível gerar os relatórios em formato HTML e CSV.

3.7.16 Possuir base de dados interna para armazenamento dos eventos.

3.7.17 Deve ser capaz de interpretar eventos em um ambiente heterogêneo, constituído de produtos de fabricantes distintos, conforme relação minima abaixo:

3.7.17.1 Sempre que for nomeado um produto na lista abaixo, a solução deverá interpretar os logs do produto de forma específica, com entendimento de

seus diversos campos, não sendo aceita solução que os interprete de forma genérica por meio de syslog ou equivalente.

3.7.17.2 Roteadores e switches

3.7.17.2.1 Switches da família CISCO 4500, Cisco 3560 e Cisco 2960, utilizadas pelo TJCE;

3.7.17.3 Firewalls

3.7.17.3.1 Solução de firewall fornecida pela CONTRATADA ;

3.7.17.3.2 Check Point NG e Firewall-1 (Atualmente em uso pelo TJCE);

3.7.17.3.3 Pelo menos duas outras soluções de firewall de fabricantes distintos do fornecido pela CONTRATADA;

3.7.17.4 Dispositivos de IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) de Rede

3.7.17.4.1 Solução de IPS fornecida pela CONTRATADA;

3.7.17.4.2 ISS RealSecure Sensor (Utilizado pelo TJCE no segmento Internet);

3.7.17.4.3 Solução de software livre Snort;

3.7.17.4.4 Pelo menos duas outras soluções de IPS de fabricantes distintos dos acima solicitados;

3.7.17.5 IDS de Servidor/Estação

3.7.17.5.1 ISS RealSecure Host Sensor;

3.7.17.6 Anti-vírus

3.7.17.6.1 Karsperky ou Symantec ou Trend Micro;

3.7.17.7 Exame de Vulnerabilidade

3.7.17.7.1 Soluções de analise de vulnerabilidades como eEye REM, Qualys QualysGuard ou outras soluções de mercado;

3.7.17.8 Sistemas Operacionais para Servidor

3.7.17.8.1 Windows

3.7.17.8.2 Redhat Linux

3.7.17.9 Servidores Web

3.7.17.9.1 Microsoft Internet Information Server

3.7.17.9.2 Apache

3.7.17.10 Servidores de Banco de Dados

3.7.17.10.1 Oracle Database

3.7.17.11 Servidores de Autenticação do tipo AAA

3.7.17.11.1 Microsoft Internet Authentication Service (IAS) Server (Solução utilizada atualmente pelo TJCE);

3.7.17.11.2 Cisco Secure Access Control Sever (ACS) (Solução de Switches utilizada pelo TJCE);

3.7.17.12 Servidores SNMP e Syslog

3.7.17.12.1 Qualquer solução que gere eventos nos padrões acima;

3.7.17.12.2 Dispositivos que gerem eventos por meio de SNMP ou Syslog;

3.7.18 Caso a solução proposta seja licenciada pela quantidade de ativos, a licitante deve considerar os seguintes quantitativos mínimos:

3.7.18.1 Switches Cisco: 500

3.7.18.2 Firewalls: 02 Checkpoint e 220 da solução fornecida

3.7.18.3 IPS: 01 ISS, 02 da solução fornecida e 04 baseados em software livre

3.7.18.4 IDS de servidor: 05 ISS

3.7.18.5 Antivírus: 04 servidores Karsperky com 5.500 estações de trabalho

3.7.18.6 Sistema operacionais: 300 Windows server, 50 Linux

3.7.18.7 Servidores Web: 100 IIS, 40 Apache

3.7.18.8 Banco de dados Oracle: 04

3.7.18.9 Servidores de autenticação IAS: 04

3.7.18.10 Servidores SNMP e Syslog: 300

## 3.8 CÓDIGO 08: Serviços de Operação Gerenciada

3.8.1 A CONTRATADA será responsável pela operação remota da solução de segurança ofertada, na modalidade 24x7x365, pelo período de até 12 (doze) meses;

3.8.2 O Tribunal de Justiça poderá a qualquer momento solicitar a interrupção da prestação dos serviços de operação gerenciada, por meio de comunicação formal à CONTRATADA com antecedência mínima de 30 (trinta) dias;

3.8.3 A CONTRATADA será responsável pelas seguintes atividades de operação gerenciada:

3.8.3.1 Gerenciamento, suporte e monitoração remota de Firewall/VPN, IPS e Correlacionador de eventos via VPN. Visitas técnicas, quando necessárias, estarão restritas às localidades com equipamentos instalados pela CONTRATADA;

3.8.3.2 Criação e manutenção de regras de Firewall/VPN e IPS;

3.8.3.3 Elaboração de análise de risco para cada inclusão/exclusão ou alteração de regra a fim de garantir a gestão de mudanças no ambiente do Tribunal de Justiça;

3.8.3.4 Criação e manutenção de contas e grupos de VPN;

3.8.3.5 Monitoração em tempo real de eventos de risco (intrusão, disponibilidade, falhas de acesso importantes etc.), com processo previamente formalizado de resposta a incidentes originados da Internet;

3.8.3.6 Análise de logs de Firewall/VPN, IPS e Correlacionador de Eventos, com geração mensal de relatórios operacionais e gerenciais para o Tribunal de Justiça, classificando todos os eventos por nível de criticidade com descrição detalhada dos eventos e recomendações de ações;

3.8.3.7 Análise dos registros dos equipamentos gerenciados, com disponibilização de relatórios contendo o resumo das principais ocorrências de segurança do mês, medidas preventivas e corretivas realizadas e recomendações de ajustes fora do escopo dos serviços gerenciados;

3.8.3.8 Atualização de patches e novas versões nos ativos do escopo desta proposta;

3.8.3.9 Nos serviços de firewall, a CONTRATADA deverá responsabilizar-se pela gravação de dados para auditoria, de forma detalhada para cada conexão efetivada, incluindo a origem, serviço, hora de conexão, destino e ação executada;

3.8.3.10 Reuniões presenciais mensais sobre o ambiente, visando a análise dos principais eventos do período e definição de ações de melhoria contínua do ambiente;

3.8.3.11 A CONTRATADA deverá prover acesso para o CONTRATANTE, no mínimo, das seguintes informações de segurança por meio da Console de gerenciamento dos firewalls:

3.8.3.11.1 Informações para todas as conexões com regras e auditoria:

3.8.3.11.1.1 Número da regra;

3.8.3.11.1.2 Data e Hora;

3.8.3.11.1.3 Endereço IP de origem;

3.8.3.11.1.4 Endereço IP de destino;

3.8.3.11.1.5 Endereço do NAT (caso exista NAT na regra);

3.8.3.11.1.6 Protocolo;

3.8.3.11.1.7 Ação (permitido, bloqueado, etc.);

3.8.3.11.1.8 Geração de logs;

3.8.3.11.1.9 Número da porta;

3.8.3.11.2 Informações de status:

3.8.3.11.2.1 Uso de processador;

3.8.3.11.2.2 Uso de memória;

3.8.3.11.2.3 Uso de disco;

3.8.3.11.2.4 Quantidade de sessões ativas;
3.8.3.11.2.5 Quantidade de pacotes em cada interface;
3.8.3.11.2.6 Nó ativo (caso exista alta disponibilidade);
3.8.3.11.2.7 Uptime;

3.8.3.11.3 Informações da política de segurança:
3.8.3.11.3.1 Lista das Regras;
3.8.3.11.3.2 Endereço IP da cada interface;
3.8.3.11.3.3 Implementação de anti-spoofing;
3.8.3.11.3.4 Objetos (hosts, networks, protocolos, usuários, etc);
3.8.3.11.3.5 Configuração de logs;

3.8.4 Acordo de Níveis de Serviço (ANS)

3.8.4.1 A CONTRATADA deverá cumprir Acordo de Nível de Serviço (ANS), em regime 24x7x365, conforme tabela abaixo. A empresa deverá apresentar, juntamente com sua proposta, declaração de que cumpre o Acordo de Nível de Serviço (ANS) especificado no item 3.8.4.

3.8.4.2 Descrição dos Indicadores:

3.8.4.2.1 Tempo de atendimento: Tempo entre o acionamento da CONTRATADA e inicio das atividades demandadas;

3.8.4.2.2 Tempo de solução: Tempo entre o início do atendimento da demanda, conforme tempo de atendimento, quando existente, e o restabelecimento/implementação do serviço, ou tempo entre o acionamento da CONTRATADA e o restabelecimento/implementação do serviço, quando tempo de atendimento não se aplica à situação;

3.8.4.3 Descrição das Categorias de Serviço:

3.8.4.3.1 Incidente: Todo e qualquer evento que não faz parte da operação normal de um serviço e que cause ou venha causar uma interrupção, ou redução da qualidade de serviço (exemplos: falha em componente de hardware, assinatura de IPS desatualizada, serviço indisponível, degradação de desempenho, ataques etc.);

3.8.4.3.1.1 Produção impactada: Serviço degradado, mas em funcionamento, permitindo a operação do negócio (exemplo: falha de uma fonte de um equipamento com redundância; desempenho de um equipamento abaixo do habitual, mas ainda dentro do aceitável; falha de um membro de uma solução de firewall redundante etc.);

3.8.4.3.1.2 Produção parada: Serviço indisponível inviabilizando as operações ou sem desempenhar seu papel previsto (exemplo: todas as fontes queimadas, indisponibilidade dos dois membros de uma solução de firewall etc.);

3.8.4.3.1.3 Segurança comprometida: Serviço violado por ataque intencional ou não, que tenha exposto o ambiente para terceiros não autorizados.

3.8.4.3.2 Requisição de serviço: Solicitações que demandem alterações no ambiente objetivadas a atender uma nova realidade ou necessidade da operação ou negócio (exemplos: alterações de regras do Firewall/VPN, ativação/desativação de assinaturas e regras de IPS, emissão de relatórios, reset de senhas, aplicações de patches etc.);

3.8.4.3.2.1 Condição para operação/negócio: Referem-se às requisições de serviço que se não implementadas inviabilizam ou podem vir a inviabilizar a operação ou negócio (exemplo: criação de regra de firewall para debug de uma aplicação que esteja fora do ar, aplicação de atualização de alta criticidade etc.);

3.8.4.3.2.2 Mudança/Melhorias no Ambiente: Referem-se às requisições de serviço que venham ser realizadas para melhorar a qualidade dos serviços prestados, bem como implementação de mudanças rotineiras do ambiente (exemplo: atualização de senhas, ajustes finos de regras,