Conselho da Justiça Federal

PROCESSO CJF – ADM 2012/00420

PREGÃO ELETRÔNICO n. 26/2013

MENOR PREÇO

OBJETO: CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE SEGURANÇA.

DATA DA ABERTURA DA SESSÃO: 16/07/2013, às 14h00min.

Conselho da Justiça Federal

PROCESSO CJF – ADM 2013/00170

MENOR PREÇO

O **CONSELHO DA JUSTIÇA FEDERAL**, por intermédio do Pregoeiro, designado pela Portaria nº. 183 de 15 de outubro de 2010, torna público, para ciência dos interessados, que às **14:00 horas**, hora de Brasília, do dia **16 de julho de 2013**, por meio do endereço eletrônico WWW.COMPRASNET.GOV.BR ou, caso não haja expediente nesta data, no primeiro dia útil subsequente, fará realizar licitação na modalidade de PREGÃO ELETRÔNICO do tipo **MENOR PREÇO**, utilizando os recursos de tecnologia da informação - Internet. O procedimento licitatório obedecerá integralmente às disposições contidas na Lei n. 10.520, de 17 de julho de 2002, e no Decreto n. 5.450, de 31 de maio de 2005, e subsidiariamente, na Lei n. 8.666, de 21 de junho de 1993, e às condições e exigências estabelecidas neste Edital.

1 – DO OBJETO

1.1 A presente licitação tem por objeto a Contratação de solução integrada de segurança, contemplando o fornecimento de equipamentos, softwares e sistemas de gerenciamento da solução, com garantia de 48 meses e serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades do Conselho da Justiça Federal - CJF, de acordo com as especificações técnicas contidas nos Módulos: I - Termo de Referência e seus Anexos e II – Especificação do Serviço/Planilha.

1.2 - Em caso de discordância existente entre as especificações do serviço descritas no COMPRASNET e as especificações constantes deste Edital, prevalecerão as últimas.

2 – DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1 A sessão deste pregão será pública e realizada em conformidade com este edital na data, no horário e no endereço eletrônico indicados no preâmbulo.

2.2 Poderão participar deste pregão eletrônico as empresas que atendam às condições deste edital e seus anexos, inclusive quanto à documentação, e estejam devidamente credenciadas na Secretaria de Logística e Tecnologia da Informação (SLTI), do Ministério do Planejamento, Orçamento e Gestão, por meio do sítio **WWW.COMPRASNET.GOV.BR**, para acesso ao sistema eletrônico, em conformidade com o inc. I do art. 13 do Decreto n. 5450/2005.

2.3 A SLTI atuará como órgão provedor do sistema eletrônico.

2.4 Como requisito para participação no pregão eletrônico, a licitante deverá manifestar, em campo próprio do sistema eletrônico, pleno conhecimento e atendimento às exigências de habilitação do presente edital.

2.5 Não poderão participar desta licitação:

a) as empresas impedidas e as suspensas de licitar ou contratar com a Administração, bem como as declaradas inidôneas, nos termos do artigo 7º da Lei n. 10.520/2002 e do artigo 87, incisos III e IV, da Lei n. 8.666/1993.;

b) servidor ou dirigente de órgão ou entidade contratante ou responsável pela licitação.

2.6 Os documentos apresentados nesta licitação deverão:

a) estar em nome da licitante, com um único número de CNPJ, com exceção:

a.1) da Certidão Negativa, ou Positiva com Efeitos de Negativa, de Débitos Relativos às Contribuições Previdenciárias e às de Terceiros, expedida pela Secretaria da Receita Federal do Brasil, e do Certificado de Regularidade do FGTS, emitido pela Caixa Econômica Federal, que poderão ser da sede da pessoa jurídica;

a.2) da Certidão de falência/concordata/recuperação judicial e da Certidão Conjunta Negativa, ou Positiva com Efeitos de Negativa, de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal do Brasil, que deverão ser da sede da pessoa jurídica;

b) estar no prazo de validade estabelecido pelo órgão expedidor;

c) ser apresentados em original, em publicação da imprensa oficial ou em cópia autenticada por cartório ou por servidor qualificado como pregoeiro;

d) vir acompanhados de tradução para a língua portuguesa, feita por tradutor juramentado, no caso de documentos apresentados em outros idiomas.

2.7 Quando se tratar de certidões vencíveis em que a validade não esteja expressa, os documentos expedidos nos últimos seis meses que antecederem à data da sessão deste certame serão considerados válidos.

3 – DO CREDENCIAMENTO DOS REPRESENTANTES

3.1 A licitante deverá credenciar-se no sistema "Pregão Eletrônico", no sítio **www.comprasnet.gov.br**, observados os seguintes aspectos:

a) o credenciamento far-se-á mediante atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico;

b) a perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema, para imediato bloqueio de acesso;

c) o credenciamento da licitante ou de seu representante perante o provedor do sistema implicará responsabilidade legal pelos atos praticados e presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

3.2 O uso da senha de acesso ao sistema eletrônico é de inteira e exclusiva responsabilidade da licitante, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.3 A licitante responsabilizar-se-á por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos durante a sessão pública.

4 – DO ENVIO DA PROPOSTA ELETRÔNICA DE PREÇOS

4.1 A participação no pregão eletrônico ocorrerá mediante digitação de senha privativa da licitante e subsequente encaminhamento da proposta de preços, discriminando o valor unitário e total para o item cotado, com base no Anexo Único deste Edital.

4.2 Após a fase de lances, por ocasião da aceitação das propostas, a licitante vencedora deverá encaminhar **proposta de preços** contendo a(s) especificação(ões) detalhada(s) do serviço, o valor unitário e total, bem como os prazos de validade e de execução do serviço, no que for aplicável, em **conformidade com o Módulo II deste Edital**, exclusivamente por meio eletrônico, no prazo de duas hora, podendo ser prorrogado pelo pregoeiro.

4.3 O não envio da proposta nos termos previstos no item 4.2 implicará a desclassificação da licitante.

4.4 Até a abertura da sessão, a licitante poderá retirar ou substituir a proposta anteriormente apresentada.

4.5 A licitante deverá acompanhar as operações no sistema eletrônico durante a sessão pública deste pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de desconexão.

5 – DA ABERTURA DAS PROPOSTAS

5.1 No dia e hora indicados no preâmbulo deste edital, o pregoeiro abrirá a sessão pública na internet, mediante utilização da chave de acesso e da senha.

5.2 As licitantes interessadas poderão participar da sessão pública na internet, por meio do uso dos recursos de acesso ao sistema eletrônico.

5.3 As propostas de preços contendo os valores estarão disponíveis na internet.

5.4 A comunicação entre o pregoeiro e as licitantes ocorrerá mediante troca de mensagens, em campo próprio do sistema eletrônico.

6 – DA FORMULAÇÃO DOS LANCES

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

6.2 Classificadas as propostas, o pregoeiro dará início à fase competitiva, momento em que as licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico.

6.3 A licitante será imediatamente informada do recebimento do lance e do respectivo valor consignado no registro.

6.4 Na formulação de lances, deverão ser observados os seguintes aspectos:

a) as licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão e as regras estabelecidas neste edital;

b) a licitante somente poderá oferecer lance inferior ao último por ela ofertado e registrado pelo sistema;

c) não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro.

6.5 Durante a sessão pública deste certame, as licitantes serão informadas em tempo real do valor do menor lance registrado, vedada a identificação do detentor.

6.6 No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva, o sistema eletrônico poderá permanecer acessível às licitantes para recepção dos lances, retornando o pregoeiro, quando possível, a atuar no certame, sem prejuízo dos atos realizados.

6.7 Quando a desconexão persistir por tempo superior a dez minutos, a sessão do pregão será suspensa e terá reinício somente após comunicação expressa aos participantes.

6.8 A etapa de lances da sessão pública será encerrada por decisão inicial do pregoeiro mediante aviso de fechamento iminente.

6.9 O sistema eletrônico encaminhará aviso de fechamento iminente dos lances, depois do qual transcorrerá período de tempo de até trinta minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

6.10 Será observado, o disposto nos artigos 44 e 45 da Lei Complementar n. 123, de 14 de dezembro de 2006.

6.11. Será assegurada, ainda, preferência na contratação, nos termos do disposto no art. 3º da Lei nº 8.248, de 23 de outubro de 1991 e do Decreto n. 7.174, de 12 de maio de 2010, para fornecedores de bens e serviços, observada a seguinte ordem:

a) bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

b) bens e serviços com tecnologia desenvolvida no País; e

c) bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal.

6.12 As microempresas e empresas de pequeno porte que atendam ao disposto no subitem 6.11 terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo subitem.

6.13 O exercício do direito de preferência disposto no subitem 6.11, será concedido, observando-se os seguintes procedimentos, sucessivamente:

a) aplicação das regras de preferência para as microempresas e empresas de pequeno porte dispostas no Capítulo V da Lei Complementar n. 123, de 2006, quando for o caso;

b) aplicação das regras de preferência previstas no subitem 6.11, com a classificação dos licitantes cujas propostas finais estejam situadas até dez por cento acima da melhor proposta válida, conforme o critério de julgamento, para a comprovação e o exercício do direito de preferência;

c) convocação dos licitantes classificados que estejam enquadrados no subitem 6.11, na ordem de classificação, para que possam oferecer nova proposta ou novo lance para superar a melhor proposta válida, caso em que será declarado vencedor do certame;

d) caso a preferência não seja exercida na forma da alínea "c", por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas na alínea "b" do subitem 6.11, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para a alínea "c" do subitem 6.11, caso esse direito não seja exercido;

e) caso nenhuma empresa classificada venha a exercer o direito de preferência, observar-se-ão as regras usuais de classificação e julgamento previstas na Lei n. 8.666, de 21 de junho de 1993, e na Lei n. 10.520, de 17 de julho de 2002.

6.13.1 Após o término da sessão pública, as empresas licitantes deverão permanecer logadas no Sistema Eletrônico para que o Pregoeiro possa convocar, na ordem de classificação e por meio do Chat, as empresas cujo valor da proposta para o item esteja situado no intervalo percentual previsto na alínea "b" do subitem 6.13, ou seja, até dez por cento da melhor proposta válida.

6.13.2 Será encaminhado às licitantes, via Chat do Sistema Eletrônico, questionamento visando identificar aquelas que porventura preencham as condições listadas no subitem 6.11.

6.13.3 Após convocada pelo Chat para informar qual das condições listadas no subitem 6.11 sua proposta atende, a empresa licitante terá o prazo de 5 (cinco) minutos para resposta, sob pena de preclusão do seu direito de preferência.

6.13.4 Na hipótese de mudança da licitante classificada em 1º lugar, em razão de manifestação de atendimento a alguma das condições listadas no subitem 6.11, a mesma será convocada, pelo Chat, e terá o prazo de 5 (cinco) minutos para apresentar proposta igual ou inferior à da licitante que apresentou originalmente o melhor lance, sob pena de preclusão do seu direito de referência.

6.14 A comprovação do atendimento ao PPB ou aos bens e serviços com tecnologia desenvolvida no País será feita mediante apresentação do documento comprobatório da habilitação à fruição dos incentivos fiscais regulamentados pelo Decreto no 5.906, de 26 de setembro de 2006, ou pelo Decreto no 6.008, de 29 de dezembro de 2006.

6.14.1 A comprovação será feita:

a) eletronicamente, por meio de consulta ao sítio eletrônico oficial do Ministério da Ciência e Tecnologia ou da Superintendência da Zona Franca de Manaus - SUFRAMA; ou

b) por documento expedido para esta finalidade pelo Ministério da Ciência e Tecnologia ou pela SUFRAMA ou por outro órgão ao qual seja atribuída tal competência, mediante solicitação da licitante.

6.15 Na hipótese em que nenhuma das licitantes preencha os requisitos elencados no subitem 6.11, prevalecerá o resultado inicialmente apurado pelo sistema eletrônico.

6.16 Após o encerramento da etapa de lances da sessão pública, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta à licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes das previstas neste edital.

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

6.18 O pregoeiro verificará, de imediato, as condições de habilitação da licitante detentora da melhor oferta.

7 – DA HABILITAÇÃO

7.1 Para habilitação neste pregão eletrônico, serão verificados: o registro cadastral atualizado no SICAF, que será confirmado por meio de consulta on-line ao sistema durante a sessão; e a documentação complementar especificada neste edital. Aos licitantes inscritos no SICAF, cuja documentação encontrar-se vencida no referido Sistema, será facultada a apresentação da documentação atualizada, no momento da habilitação.

7.2 Os dados dos documentos de habilitação registrados no SICAF a serem avaliados são os seguintes:

a) número da inscrição no Cadastro Nacional de Pessoa Jurídica - CNPJ do Ministério da Fazenda;

b) Certidão Conjunta Negativa, ou Positiva com Efeitos de Negativa, de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal do Brasil;

c) Certidão Negativa, ou Positiva com Efeitos de Negativa, de Débitos Relativos às Contribuições Previdenciárias e às de Terceiros, expedida pela Secretaria da Receita Federal do Brasil;

d) Prova de regularidade com a Fazenda Estadual/Distrital e a Fazenda Municipal, no caso de empresas de fora de Brasília.

e) CRF - Certificado de Regularidade do FGTS, emitido pela Caixa Econômica Federal.

7.2.1 Será verificado, por meio de consulta ao SICAF, se na composição societária da licitante vencedora há servidores do CJF, o que constitui fato impeditivo de contratação com este Órgão.

7.3 Será também verificada a existência de registros impeditivos de contratação no Cadastro Nacional de Empresas Inidôneas e Suspensas/CGU, disponível no Portal da Transparência

(http://portaltransparencia.gov.br) e no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa disponível no Portal do Conselho Nacional de Justiça (CNJ) (www.cnj.jus.br), em atendimento ao disposto no Acórdão 1793/2011 do Plenário do Tribunal de Contas da União.

7.4 Será exigida, ainda, a Certidão Negativa de Débitos Trabalhistas (CNDT), instituída pela Lei n. 12.440, de 7 de julho de 2011.

7.5 Para fins de habilitação e em cumprimento ao subitem 9.1, deverão ser apresentados ainda:

a) ATESTADO DE CAPACIDADE TÉCNICA, emitido por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove ter a LICITANTE fornecido e implementado a contento, para órgão ou entidades públicas ou privadas, solução englobando o fornecimento de firewall de rede ou firewall de aplicação e analisador de vulnerabilidades, composta por vários equipamentos ou apenas por um que atenda a essas funcionalidades, nos termos da Lei.

a.1) Deverão constar, preferencialmente, do atestado de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato , local e data de expedição, data de início e término do contrato.

b) Declaração de cumprimento do disposto no artigo 7º, XXXIII, da Constituição Federal/1988, e artigo 27, inciso V, da Lei n. 8.666/1993.

c) Declaração de Fato Superveniente, se for o caso, que impeça a sua habilitação, assinada por seu representante ou procurador, devidamente identificado;

d) Declaração de Garantia comprometendo-se a prestar garantia de, no mínimo, 48 (quarenta e oito) meses a contar da data de recebimento do Termo de Recebimento Definitivo (TRD);

e) Declaração de Suporte Técnico comprometendo-se a prestar suporte pelo período mínimo de 48 (quarenta e oito) meses a contar da data de recebimento do Termo de Recebimento Definitivo (TRD);

f) Certidão Negativa de Falência ou, se for o caso, Certidão de Recuperação Judicial, expedida pelo Cartório Distribuidor da sede da pessoa jurídica;

g) registro comercial, no caso de empresa individual;

h) ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades empresariais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores e alterações ou da consolidação respectiva;

7.6 Caso nos registros cadastrais conste algum documento com prazo de validade vencido, a licitante deverá encaminhar comprovante idêntico, com o respectivo prazo atualizado, no prazo e condições estipulados no subitem 9.1, sob pena de inabilitação.

7.7 A licitante que apresentar documentação em desacordo com este edital será inabilitada.

7.8 Conforme regem os artigos 42 e 43, da Lei Complementar n. 123, de 14 de dezembro de 2006, as microempresas e empresas de pequeno porte, por ocasião da participação no certame, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

7.8.1 Será consultado o portal da transparência do Governo Federal, para verificação do faturamento máximo disposto no art. 3º da Lei Complementar n. 123, de 2006, em observância do tratamento jurídico diferenciado previsto na referida legislação a ser atribuído às licitantes declaradas como microempresa e empresa de pequeno porte.

7.8.2 Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de dois dias úteis, cujo termo inicial corresponderá ao momento em que a licitante for declarada vencedora do certame, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

7.8.3 A não-regularização da documentação no prazo previsto no subitem 7.8.2, implicará decadência do direito à contratação, sem prejuízo das sanções legalmente previstas, quando serão convocadas as licitantes remanescentes, na ordem de classificação.

8 – DO JULGAMENTO DAS PROPOSTAS E DA PROVA DE CONCEITO

8.1 Na hipótese de a proposta ou o lance de menor valor não serem aceitos ou se a licitante detentora da melhor proposta desatender às exigências habilitatórias, o pregoeiro examinará a proposta ou o lance subsequente, verificando a sua aceitabilidade e procedendo à sua habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de proposta ou lance que atenda ao edital.

8.2 Serão desclassificadas as propostas de preços que não atenderem às exigências deste edital;

8.3 Será declarada vencedora a licitante que apresentar o **menor preço global** e que cumprir todos os requisitos de habilitação.

8.4. Da Prova de Conceito

8.4.1. Poderá ser solicitada, a critério exclusivo do CJF, prova de conceito da solução integrada de segurança à empresa classificada em primeiro lugar após a fase de lances, com o objetivo de realizar testes de comprovação de atendimento às especificações e requisitos exigidos nas Especificações Técnicas do Módulo I - Termo de Referência, caso a documentação entregue pela LICITANTE seja considerada insuficiente para comprovar o atendimento a todos os itens exigidos.

8.4.2. Para a realização da prova de conceito da solução integrada de segurança, a LICITANTE deverá disponibilizar conjunto de elementos que atendas as funcionalidades de gerenciamento de ameaças, gestão de vulnerabilidades e firewall de aplicação, devendo ser da mesma marca, modelo e especificações detalhadas na proposta.

8.4.3. A realização da prova de conceito deverá ser presencial e realizada, preferencialmente, na Secretaria de Tecnologia da Informação do CJF, localizada no SCES Trecho 03 Pólo 08 Lote 09, CEP 70200-003, Brasília - DF, em dias úteis, ou, a critério exclusivo do CJF e mediante exposição de motivos, em qualquer cidade brasileira, devendo iniciar no prazo de até 05 (cinco) dias úteis, contados a partir da data de convocação do CJF para a realização da prova de conceito.

8.4.4. O CJF, a seu critério, poderá prorrogar a duração da prova de conceito por mais 02 (dois) dias úteis.

8.4.5. A prova de conceito utilizará como base as especificações técnicas constantes do Módulo I - Termo de Referência deste Edital.

8.4.6. Será rejeitada a prova de conceito que:

a) Não comprovar o atendimento de, pelo menos, 01 (um) requisito técnico descrito no ANEXO I - Especificações Técnicas do Módulo I – Termo de Referência, executada nos equipamentos e softwares entregues para a prova de conceito.

b) Apresentar divergências entre as especificações dos equipamentos e softwares entregues para a prova de conceito em relação às especificações técnicas da proposta entregue pela LICITANTE.

8.4.7. Não será aceita a proposta da LICITANTE que tiver a prova de conceito rejeitada ou não entregue no prazo estabelecido.

Conselho da Justiça Federal

8.4.8. Nesse caso, a proposta subsequente será examinada e, assim, sucessivamente, na ordem de classificação, até a aprovação de uma prova de conceito.

9 – DO ENVIO DA PROPOSTA DE PREÇOS E DA DOCUMENTAÇÃO DE HABILITAÇÃO DA LICITANTE VENCEDORA

9.1 Após aceitação da proposta, os documentos de habilitação constantes do Item 7 deverão ser encaminhados ao pregoeiro, para o endereço eletrônico cpl@cjf.jus.br, **no prazo de duas horas, contado da solicitação no sistema eletrônico.**

9.2 A proposta de preços e os documentos de habilitação também deverão ser apresentados em documento original ou em cópia autenticada por cartório ou por servidor qualificado como pregoeiro, remetidos ao endereço SCES, Lote 09, Trecho 03, Pólo 08, Sala 105, CPL, Brasília – DF, CEP: 70.200-003, **no prazo de três dias úteis**, **contado da sessão de encerramento do certame.**

9.3 Para garantir a integridade da documentação e da proposta, recomenda-se que contenham índice e folhas numeradas e timbradas com o nome, logotipo ou logomarca da licitante.

9.4 A proposta de preços deverá ser redigida em língua portuguesa, datilografada ou impressa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverão constar:

a) identificação social, número do CNPJ, assinatura do representante da proponente, referência a esta licitação, número de telefone, endereço, dados bancários, fac-símile e, se houver, indicação de endereço eletrônico (e-mail);

b) as especificações de forma clara e detalhada da solução cotada, e deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item;

c) em qual página e item da documentação apresentada, está a comprovação do atendimento dos requisitos técnicos descritos no ANEXO I do Módulo I - Termo de Referência.

c.1) Todos os equipamentos e softwares especificados deverão ser adquiridos em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo com o término do contrato;

d) indicação única de preço para o item, com exibição do valor unitário e total em algarismos e o valor total da proposta em algarismos e por extenso, com duas casas decimais, conforme o lance final respectivo, podendo as licitantes elaborarem suas propostas com base no modelo do Módulo II deste Edital;

e) prazo de validade da proposta não inferior a **60 (sessenta) dias**, contado da data da sessão pública de recebimento da proposta de preços.

f) prazo de entrega dos equipamentos, licenças de softwares e acessórios que não poderá ser superior a 45 (quarenta e cinco) dias, contados da emissão da Ordem de Serviço, conforme descrito no item 5.2 do Módulo I – Termo de Referência e seu Anexo III Cronograma de Implantação;

g) prazo de garantia e suporte técnico da solução que não poderá ser inferior a 48 (quarenta e oito) meses, contados da data de recebimento do Termo de Recebimento Definitivo (TRD);

g.1) as condições da garantia e do Suporte técnico estão descritas nos itens 5.4 e 5.5 do Módulo I;

h) que realizará a Transferência de Conhecimento**,** com carga horária mínima de 80 (oitenta) horas, conforme descrito no item 5.3 do Módulo I.

h.1) a Transferência de Conhecimento será realizada em Brasília/DF e a licitante deverá providenciar as instalações para o treinamento.

Conselho da Justiça Federal

9.5. Quando da elaboração da proposta, as licitantes deverão considerar ainda os seguintes requisitos:

a) O conjunto dos requisitos especificados para as Soluções: de Gerenciamento de Ameaças, de Gestão de Vulnerabilidades e de Firewall de Aplicação poderá ser atendido:

a.1) por meio de um único equipamento: ou

a.2) pela composição dos equipamentos, produtos, peças e softwares que os compõem, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança;

b) o profissional que atuará do início da execução do Contrato até a conclusão da implantação como Gerente de Projeto, deverá possuir certificação PMP (Project Management Professional).

9.6. A licitante deverá fornecer os equipamentos e softwares da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CJF, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração.

9.7. Os modelos e versões dos equipamentos (hardware) que compõe a solução integrada de segurança deverão ser ofertados novos, sem uso anterior, e deverão permanecer em linha de produção pelos próximos 12 (doze) meses, contados da entrega dos equipamentos, e com previsão de suporte pelos próximos 5 (cinco) anos, contados da data de assinatura do Contrato.

9.8. A solução integrada de segurança deverá operar de forma integrada, ou seja, os equipamentos, softwares fornecidos e configurações aplicadas pela licitante deverão operar como um conjunto plenamente ajustado, de forma a garantir desempenho, disponibilidade e funcionalidades adequados aos requisitos do Conselho.

9.9. A solução integrada de segurança será composta por elemento de gerenciamento de ameaças, elemento de gestão de vulnerabilidades e elemento firewall de aplicação, englobando todos os softwares e sistemas de gerenciamento, necessários para seu completo funcionamento, que deverão ser integrados ao ambiente tecnológico do CJF (detalhado no ANEXO II do Módulo I-Termo de Referência).

9.10. A Licitante caso julgue conveniente para o correto dimensionamento e cumprimento das obrigações, poderá realizar vistoria nas instalações do CJF para tomar conhecimento dos serviços a serem realizados, conforme modelo fornecido no Módulo IV - Termo de Vistoria.

9.10.1. As vistorias deverão ser realizadas em dias úteis, no horário de 9:00 às 11:00 e das 14:00 às 17:00, até 1 (um) dia antes da abertura da licitação, no endereço do Conselho da Justiça Federal, em Brasília-DF. O agendamento das vistorias deverá ser feito pelo telefone (61) 3022-7400 ou 3022-7403.

9.10.2. A visita técnica deverá ocorrer por horário marcado, e será agendada pela área de infraestrutura de TI através dos telefones acima, em até 48 (quarenta e oito) horas antes da data e horário de abertura do processo licitatório.

9.10.3. Detalhes da topologia lógica da rede de dados do CJF serão apresentados durante a vistoria somente mediante assinatura de Termo de Confidencialidade e Sigilo da Licitante (ANEXO IV), a ser preenchido e assinado pelo representante legal da empresa.

9.10.4. A Vistoria não é obrigatória, porém não se admitirá em hipótese alguma, alegações posteriores de desconhecimento dos serviços e de dificuldades técnicas não previstas, em razão da falta de sua realização.

9.11. No caso de os prazos de execução do serviço, de validade da proposta e garantia/suporte técnico serem **omitidos** na proposta, o **Pregoeiro** entenderá como sendo iguais aos previstos, respectivamente, no **item 9.4, alíneas "e", "f" e "g".**

9.12. O preço proposto no lance final será fixo e irreajustável e nele deverão estar incluídos os tributos e demais encargos.

10 – DOS RECURSOS

10.1 Declarada a vencedora, qualquer licitante poderá manifestar imediata **motivadamente** a intenção de recorrer durante a sessão pública, em campo próprio no sistema eletrônico.

10.2 A falta de manifestação imediata e motivada da licitante implicará decadência do direito de recurso.

10.3 A recorrente deverá apresentar as razões do recurso no prazo de três dias, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões em igual prazo, que começará a correr do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

10.3.1 No caso de apresentação de razões e contrarrazões via fax, as licitantes deverão apresentar os documentos originais no prazo indicado no item anterior.

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

10.5 Os autos do processo permanecerão com vista franqueada aos interessados.

10.6 - Além do recurso previsto no item 10.1, dos atos do Pregoeiro ou da Autoridade Competente ainda cabem:

10.6.1. recurso, no prazo de 05 (cinco) dias úteis, a contar da intimação do ato nos casos de: I - anulação ou revogação da licitação; II – rescisão do contrato a que se refere o inciso I do art. 79 da Lei nº 8.666/93; III - aplicação das penas de advertência, suspensão temporária de participação em licitação ou multa, conforme a Lei nº 8.666/93;

10.6.2. representação, no prazo de 05 (cinco) dias úteis da intimação da decisão relacionada com o objeto da licitação ou da Ata, de que não caiba recurso hierárquico;

10.6.3. pedido de reconsideração, da decisão do Ministro Presidente do CJF, no caso de aplicação de pena de declaração de inidoneidade para licitar ou contratar com a Administração, no prazo de 10 (dez) dias úteis contados da intimação do ato.

10.7 O recurso será dirigido à autoridade superior por intermédio do Pregoeiro, podendo este reconsiderar sua decisão no prazo de 05 (cinco) dias úteis ou, nesse mesmo prazo, fazê-lo subir, devidamente informado. Nesse caso, a decisão deverá ser proferida no prazo de 05 (cinco) dias úteis contados do recebimento do recurso, sob pena de responsabilidade.

11 – DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

11.1 A adjudicação do objeto será feita pelo pregoeiro à licitante vencedora e ficará sujeita à homologação pela autoridade competente do CONSELHO DA JUSTIÇA FEDERAL.

12 – DA CONTRATAÇÃO

12.1. Será firmado contrato com a licitante vencedora com base nos dispositivos da Lei nº 8.666/93 (MÓDULO III – Minuta de Contrato)**.**

12.2. O prazo para assinatura do contrato será de 05 (cinco) dias úteis, após regular convocação pelo CJF, sob pena de, não o fazendo, decair do direito à contratação sujeitando-se às penalidades previstas neste Edital.

12.3. As demais condições constam do instrumento contratual a ser celebrado com a licitante vencedora, conforme Minuta de Contrato (ANEXO III).

12.4. Por ocasião da assinatura do contrato, o CJF exigirá da licitante vencedora a apresentação dos comprovantes de regularidade do INSS (por intermédio da CND – Certidão Negativa de Débito), do FGTS (por meio do CRF – Certificado de Regularidade do FGTS), da Certidão de Quitação de Tributos e Contribuições Federais – SRF e da Certidão Quanto à Dívida Ativa da União.

12.5 - Ao assinar o Contrato a licitante vencedora obriga-se a realizar o fornecimento/serviço a ela adjudicado, conforme especificações e condições contidas neste Edital, em seus Módulos e também na proposta de preços apresentada, prevalecendo, no caso de divergência, as especificações e condições do Edital.

12.6 - É facultado ao Conselho da Justiça Federal, quando a licitante vencedora não apresentar situação regular no ato do Contrato ou recusar-se a assiná-lo no prazo e nas condições estabelecidas, convocar as licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo, ou revogar a licitação, independentemente das sanções previstas neste Edital.

12.7. Para o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventualmente aplicadas, a Contratada entregará ao CJF, no prazo máximo de 20 (vinte) dias contados da data da assinatura do contrato, garantia correspondente a 5% (cinco por cento) do valor total contratado, nos termos do artigo 56, § 2º da Lei n.º 8.666/93.

12.7.1 A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expirar o vencimento, alteração por aumento no valor do contrato ou outra necessidade indispensável.

12.8. Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ao até mesmo restrinjam-lhe a cobertura ou a sua eficácia.

12.9. O termo da garantia será restituído à CONTRATADA depois de encerrada a vigência contratual, e após o cumprimento integral de todas as obrigações contratuais.

12.10 – Quando da assinatura do Contrato também será exigido a assinatura do Termo de Confidencialidade, conforme Anexo V – do Módulo I**.**

12.11 - Decorrido os prazos de validade das propostas sem convocação para a assinatura do Contrato, ficam as licitantes liberadas dos compromissos assumidos.

13 – DAS PENALIDADES

13.1. Para os fins previstos no art. 86 e 87 da Lei 8.666/93, pela inexecução total ou parcial das obrigações assumidas a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as seguintes sanções.

13.1.1. Advertência;

13.1.2. Multa no percentual correspondente a 0,05% (cinco centésimos por cento), calculada sobre o valor total da contratação, **por dia de atraso na entrega do plano de implantação**, além do prazo máximo definido no CRONOGRAMA (ANEXO III DO MÓDULO I), até o limite de 30 (trinta) dias corridos.

13.1.3. Multa no percentual correspondente a 0,1% (um décimo por cento), calculada sobre o valor total da contratação, **por dia de atraso na entrega de todos os equipamentos, softwares e acessórios da solução**, além do prazo máximo definido no CRONOGRAMA (ANEXO III DO MÓDULO I), até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

13.1.4. Multa no percentual correspondente a 0,15% (quinze décimos por cento), calculada sobre o valor total da contratação, **por dia de atraso na conclusão da etapa de instalação e configuração da solução**, além dos prazos máximos definidos no CRONOGRAMA (ANEXO III

DO MÓDULO I) até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

13.1.5. Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total do serviço de transferência de conhecimento, **por dia de atraso na conclusão do serviço de transferência de conhecimento**, além do prazo máximo definido no CRONOGRAMA (ANEXO III DO MÓDULO I), até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

13.1.6. Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total da contratação, **no caso de aplicação de glosa referente ao mesmo indicador de Nível Mínimo de Serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses**, caracterizando inexecução parcial do contrato.

13.1.7. Multa no percentual correspondente a 0,01% por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor total do contrato, **no caso de atraso injustificado no credenciamento do representante**, constante no item 5.1.8 do Termo de Referência, Módulo I.

13.1.8. Multa no percentual correspondente a 0,20% por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor da garantia contratual disposta no item 17.1 do Termo de Referência, Módulo I, **no caso de atraso injustificado na sua entrega.**

13.1.9. A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da multa, no percentual de 20% (dez por cento) sobre o valor da parte não entregue ou não executada.

13.1.10. Multa no valor de 5% (cinco por cento), sobre o valor total da contratação, **no caso de inexecução total do contrato**.

13.1.11. O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos artigos 87 e 88 da Lei n. 8.666/1993.

13.2. O valor da multa aplicada, após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pelo CONTRATANTE, descontado da garantia contratual ou cobrado judicialmente.

13.3. A reincidência da aplicação de multa ou advertência dará direito ao CJF à rescisão contratual unilateral.

13.4. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

13.5. A critério da autoridade competente do Conselho, com fundamento nos Princípios da Proporcionalidade e Razoabilidade, as penalidades poderão ser relevadas ou atenuadas, em razão de circunstâncias fundamentadas em fatos reais e comprovados e desde que formuladas, por escrito, no prazo máximo de 05 (cinco) dias úteis, contado da data em que for oficiada da pretensão no sentido da aplicação da pena.

13.6. Quem, convocado dentro do prazo de validade da sua proposta, não assinar a Ata e celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e, será descredenciado no Sicaf, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do Art. 4º da Lei 10.520/02, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e das demais cominações legais.

13.7. Além da suspensão acima informada, a empresa que se recusar injustificadamente a assinar o Contrato, será multada em 5% (cinco por cento) do valor total da Contratação, por caracterizar descumprimento total da obrigação, com base no artigo 81 da Lei 8.666/93.

14 – DO RECEBIMENTO DO OBJETO

14.1 A entrega dos equipamentos, softwares e acessórios da solução bem como a realização dos serviços previstos neste Edital e Módulos deverão ser realizados na sede do CJF, situada no Setor de Clubes Esportivos Sul – SCES, Lote 09, Trecho 03, Pólo 08, Brasília, DF, CEP 70.200-003.

14.2 O recebimento e a Aceitação Definitiva do objeto deste pregão será realizado obedecendo ao disposto no artigo 73 a 76 da Lei n. 8.666/93, no que lhes for aplicável.

15 – DO FATURAMENTO E PAGAMENTO

15.1 O faturamento e o pagamento obedecerão ao disposto na Cláusula Sétima do Módulo III – Minuta de Contrato**.**

15.2 O CJF exigirá da licitante vencedora, por ocasião do pagamento, a apresentação dos comprovantes de regularidade junto à Secretaria da Receita Federal do Brasil, por meio da Certidão Conjunta Negativa, ou Positiva com Efeitos de Negativa, de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União e da Certidão Negativa, ou Positiva com Efeitos de Negativa, de Débitos Relativos às Contribuições Previdenciárias e às de Terceiros e junto à Caixa Econômica Federal, por meio do CRF – Certificado de Regularidade do FGTS.

15.2.1 Será exigida também a Certidão Negativa de Débitos Trabalhistas (CNDT) instituída pela Lei n.12.440, de 7 de julho de 2011.

16 – DA DOTAÇÃO ORÇAMENTÁRIA

16.1 As despesas decorrentes da execução do serviço objeto do presente pregão correrão à conta de recursos específicos consignados ao Conselho da Justiça Federal no Orçamento Geral da União.

17 – DA IMPUGNAÇÃO E DO PEDIDO DE ESCLARECIMENTO

17.1 Até dois dias úteis antes da data fixada para abertura da sessão deste pregão, qualquer pessoa poderá impugnar este ato convocatório, mediante petição a ser encaminhada ao endereço eletrônico **cpl@cjf.jus.br**.

17.1.1 No caso de apresentação de impugnações via fax ou e-mail, as licitantes deverão apresentar os documentos originais no prazo indicado no item anterior.

17.2 Caberá ao pregoeiro decidir sobre a petição no prazo de 24 horas.

17.3 Acolhida a impugnação ao ato convocatório, será designada nova data para a realização do certame.

17.4 Os pedidos de esclarecimentos relativos ao certame deverão ser enviados ao pregoeiro em até **três dias úteis** anteriores à data fixada para abertura da sessão pública, exclusivamente no endereço eletrônico **cpl@cjf.jus.br**.

17.4.1. É de responsabilidade das licitantes interessadas na licitação em consultar periodicamente o site acima indicado para verificar as impugnações e questionamentos apresentados e suas respectivas respostas.

18 – DAS DISPOSIÇÕES FINAIS

18.1 O edital estará à disposição dos interessados na Comissão Permanente de Licitação, localizada no 1º andar do Prédio Sede do CJF, telefones 3022-7510, 7511 ou 7513, nos dias úteis, de 9h às 19h, e na internet para *download,* nos endereços eletrônicos: www.comprasnet.gov.br e http://www.jf.jus.br/cjf/cjf/transparencia-publica.

18.2 Todas as referências de tempo no edital, no aviso e durante a sessão pública observarão, obrigatoriamente, o horário de Brasília – DF. Dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

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

18.4 A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do pregão constarão de ata divulgada no sistema eletrônico.

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

18.6 O pregoeiro ou a autoridade superior poderão subsidiar-se em pareceres emitidos por técnicos ou especialistas no assunto objeto desta licitação.

18.7. O objeto da presente licitação poderá sofrer acréscimos ou supressões em conformidade com o estabelecido nos § § 1º e 2º do art. 65 da Lei 8.666/93.

18.8. O Pregoeiro resolverá os casos omissos com base na legislação vigente.

18.9 As decisões do Pregoeiro serão consideradas definitivas somente após homologadas pelo Ordenador de Despesas do CJF**.**

18.10 Toda comunicação oficial ocorrerá por e-mail, pelo sítio www.comprasnet.gov.br ou por publicação, nos termos da legislação.

18.11 Na hipótese de procedimento judicial, fica eleito o foro de Brasília-DF.

Brasília, 01 de julho de 2013.

RAFAEL DE FIGUEIREDO SANTOS
Pregoeiro

Conselho da Justiça Federal

ANEXO I DO PREGÃO ELETRÔNICO n. 26/2013

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de solução integrada de segurança, contemplando o fornecimento de equipamentos, softwares e sistemas de gerenciamento da solução, com garantia de 48 meses e serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades do Conselho da Justiça Federal - CJF, de acordo com as especificações técnicas contidas no Termo de Referência.

2. (...)

3. QUANTITATIVOS

3.1. O objeto da contratação é uma solução integrada de segurança, composta por equipamentos e softwares com garantia por 48 meses, serviços de instalação e configuração, serviço de transferência de conhecimento e serviço de suporte técnico por 48 meses, contados a partir da emissão do Termo de Recebimento Definitivo.

3.2. O conjunto dos requisitos especificados para os subitens 1.1, 1.2 e 1.3 poderá ser atendido por meio de um único equipamento ou pela composição dos equipamentos, produtos, peças e softwares que os compõem, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança. Desta forma, abre-se para que o mercado defina qual a composição que melhor atende aos requisitos técnicos aqui descritos, tendo como baliza o menor custo global para a Administração.

ITEM	SUBITEM	DESCRIÇÃO	Qtd.
Único	1.1	Solução de Gerenciamento de Ameaças, com garantia por 48 meses.	01
	1.2	Solução de Gestão de Vulnerabilidades, com garantia por 48 meses.	01
	1.3	Solução de Firewall de Aplicação, com garantia por 48 meses.	01
	1.4	Serviço de Instalação e configuração da Solução.	01
	1.5	Serviço de Suporte Técnico, pelo período de 48 meses.	48
	1.6	Transferência de Conhecimento (por pessoa).	04

4. DA EXECUÇÃO DO OBJETO

4.1. A solução integrada de segurança deverá operar de forma integrada, ou seja, os equipamentos, softwares fornecidos e configurações aplicadas pela CONTRATADA deverão operar como um conjunto plenamente ajustado, de forma a garantir desempenho, disponibilidade e funcionalidades adequados aos requisitos do Conselho.

4.2. A solução integrada de segurança será composta por elemento de gerenciamento de ameaças, elemento de gestão de vulnerabilidades e elemento firewall de aplicação, englobando todos os softwares e sistemas de gerenciamento, necessários para seu completo funcionamento, que deverão ser integrados ao ambiente tecnológico do CJF (detalhado no ANEXO II).

4.3. Os modelos e versões dos equipamentos (hardware) que compõe a solução integrada de segurança deverão ser ofertados novos, sem uso anterior, e deverão permanecer em linha de produção pelos próximos 12 (doze) meses, contados da entrega dos equipamentos, e com previsão de suporte pelos próximos 5 (cinco) anos, contados da data de assinatura do Contrato.

5. OBRIGAÇÕES DA CONTRATADA

5.1 Obrigações Gerais

5.1.1 Fornecer os equipamentos e softwares da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CJF, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração.

5.1.2 Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Termo de Referência.

5.1.3 Submeter à prévia aprovação da CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.

5.1.4 Manter, durante a execução do contrato a ser firmado, as condições de habilitação e qualificação exigidas na licitação.

5.1.5 Sujeitar-se à fiscalização da CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer.

5.1.6 Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos equipamentos e softwares que compõem a solução integrada de segurança.

5.1.7 Não utilizar pessoal técnico já alocado em contratos ou projetos em execução no CONTRATANTE para prestar as atividades objeto da licitação, devendo compor equipe exclusiva para este fim.

5.1.8 Credenciar devidamente um Representante Técnico para, em todas as questões relativas ao cumprimento do objeto, representar a CONTRATADA.

5.1.9 O profissional indicado atuará desde o início da execução do contrato até a conclusão da implantação como Gerente de Projeto, devendo possuir certificação PMP (Project Management Professional).

5.1.10 Propor os ajustes necessários à adequação, segurança e racionalização dos serviços prestados, respeitando o objeto deste Termo de Referência.

5.1.11 Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias prevêem e demais exigências legais para o exercício da atividade objeto desta licitação.

5.1.12 Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação das penalidades previstas, caso os prazos e condições não sejam cumpridas.

5.1.13 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento

para cobrança de pagamentos adicionais ao CONTRATANTE ou a não prestação satisfatória dos serviços.

5.1.14 Guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE.

5.1.15 Substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado.

5.1.16 Acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1º, da Lei nº 8.666/93, as solicitações da CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto licitado.

5.1.17 Assumir a responsabilidade por danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do objeto licitado, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE.

5.1.18 Sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe de Fiscalização e Recebimento indicada pelo CONTRATANTE para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas.

5.1.19 Comunicar a Equipe de Fiscalização e Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.

5.1.20 Corrigir as falhas detectadas pela Equipe de Fiscalização e Recebimento indicada pelo CONTRATANTE.

5.1.21 Executar as atividades previstas no contrato em estrito cumprimento aos prazos previstos no ANEXO III – Cronograma de Implantação.

5.2 Quanto à entrega, instalação e configuração dos equipamentos e softwares da solução.

5.2.1 Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança de acordo com os prazos definidos no cronograma (Anexo III), contados a partir da emissão de Ordem de Serviço - OS pelo CONTRATANTE.

5.2.2 No 3º (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na SEDE do CONTRATANTE, com o objetivo de apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução integrada de segurança.

5.2.3 A CONTRATADA deverá apresentar um Plano de Implantação, em até 30 (trinta) dias da emissão da Ordem de Serviço pelo CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução integrada de segurança.

5.2.4 O Plano de Implantação deverá dispor também sobre o cronograma de execução, previsão de recursos humanos e materiais, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

a) Detalhar os procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, softwares e acessórios entregues.

b) Detalhar informações sobre as etapas de instalação física dos equipamentos, incluindo: distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e endereçamento de gerência IP.

c) Documentar a atual topologia física e lógica da rede LAN do CJF e propor nova topologia física e lógica, com base nas melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução, interligando-os aos ativos de rede existentes no CJF.

d) Planejar a engenharia de tráfego da rede CJF, com base nas melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução.

d.1) A topologia lógica a ser planejada deverá prever a existência de 3 (três) segmentos de rede a serem protegidos e monitorados.

e) Documentar regras e configurações atuais aplicadas aos ativos de segurança existentes no CONTRATANTE e planejar a aplicação destas regras e configurações nos equipamentos e softwares da solução integrada de segurança, eliminado as regras inativas ou desnecessárias, mediante aprovação do CONTRATANTE.

f) Indicar de forma detalhada as condições de *rollback* de cada mudança no ambiente do CJF.

g) Elaborar atividades de teste de operação da solução.

g.1) Elaborar planos de testes para os diversos componentes da solução que comprovem o funcionamento das regras e configurações aplicadas, bem como dos recursos de tolerância a falhas dos equipamentos e softwares da solução integrada de segurança.

5.2.5 Entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até 45 (quarenta e cinco) dias, a contar da data de emissão da Ordem de Serviço pelo CONTRATANTE.

5.2.6. Entregar os equipamentos novos e de 1º uso, no prazo indicado na alínea anterior, juntamente com todos os itens acessórios de hardware e de software necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração, conforme especificações constantes do ANEXO I deste Termo de Referência.

5.2.7 Entregar os equipamentos devidamente protegidos e embalados, originais e lacrados, os quais devem evitar danos de transporte e manuseio.

5.2.8 Desembalar os equipamentos após a entrega nas dependências do CONTRATANTE.

5.2.9 Entregar os equipamentos e softwares, à suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos.

5.2.10 Entregar todos os documentos comprobatórios de garantia indicados no item 5.4.7.

5.2.11 Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização.

5.2.12 Instalar os equipamentos e softwares nas datas e horários definidos no Plano de Implantação, sob supervisão da equipe técnica do CONTRATANTE.

5.2.13 Aceitar que as atividades de instalação, configuração dos equipamentos e softwares e operação assistida ON-SITE da solução integrada de segurança deverão

ser executadas por equipe multidisciplinar, composta por técnicos plenamente qualificados na solução que será fornecida. A equipe da CONTRATADA deverá possuir certificação emitida pelos fabricantes dos equipamentos e softwares da solução ofertada e deverá ser capaz de configurar os componentes da atual infraestrutura do CJF, conforme equipamentos, modelos e versões informados no ANEXO II - Ambiente Tecnológico do CJF.

5.2.14 Aceitar que as atividades de instalação e configuração dos equipamentos e softwares da solução integrada de segurança deverão ocorrer localmente nas dependências do CJF, devendo ser realizada em horários que não coincidam com o expediente do CONTRATANTE. O CJF poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção.

5.2.15 Aceitar que o processo de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança da solução deverá ser acompanhado pela equipe técnica indicada pelo CONTRATANTE.

5.2.16 Aceitar que caso a implantação de qualquer elemento da solução integrada de segurança cause interferência na correta operação da rede de dados do CJF, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação.

5.2.17 A execução dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança deverão contemplar, no mínimo, os seguintes itens:

a) Instalação física e ativação dos equipamentos da solução.

b) Realizar, se necessário, a movimentação de equipamentos e racks previamente existentes no Datacenter, caso este cenário implique na melhor configuração e organização do ambiente do CONTRATANTE.

c) Realizar a integração dos equipamentos da solução a rede LAN existente no CJF, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração dos equipamentos, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o CJF.

d) Instalar e configurar todas as funcionalidades exigidas na especificação técnica da solução, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do CJF.

e) Aplicar nos elementos da solução integrada de segurança todas as configurações existentes nos ativos de segurança do CONTRATANTE.

f) Realizar testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas da solução integrada de segurança.

g) Atualizar o plano de implantação com todas as informações que represente a topologia física e lógica, a configuração final e as regras aplicadas aos equipamentos e softwares da solução integrada de segurança.

5.2.18 Receber cópia do Termo de Recebimento Provisório (TRP) após entrega dos equipamentos, softwares, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no cronograma do ANEXO III. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo

máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

5.2.19 Concluir no prazo de 60 (sessenta) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação e configuração dos equipamentos e softwares da solução integrada de segurança, realizando todas as atividades programadas para esta etapa.

5.2.20 Receber cópia do Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança. O recebimento definitivo realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

5.2.21 Realizar, por 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo (TRD), operação assistida ON-SITE da solução integrada de segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução.

5.2.21.1 O serviço de operação assistida ON-SITE da solução integrada de segurança deverá ser executado presencialmente nas instalações do CJF, 8 (oito) horas por dia, durante o período normal de produção do ambiente de TI, compreendido das 07h às 20h.

5.3 Quanto ao serviço de transferência de conhecimento

5.3.1. A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE por meio de treinamento nas tecnologias da solução com carga horária total de no mínimo 80 (oitenta) horas.

5.3.2. A transferência de conhecimento deverá ser realizada em Brasília/DF, cabendo a CONTRATADA providenciar as instalações para este fim.

5.3.3 A transferência de conhecimento deverá abordar, no mínimo, as seguintes funcionalidades da solução:

a) Gerenciamento de Ameaças.

b) Filtro de Conteúdo.

c) Balanceamento de Carga.

d) Prevenção de Intrusão.

e) Gestão de Vulnerabilidades.

f) Firewall de Aplicação.

5.3.4 O programa para a transferência de conhecimento deverá ser de natureza teórica e prática, devendo abranger os equipamentos e softwares fornecidos em seus aspectos relacionados à solução implantada no ambiente computacional do Conselho, contendo, no mínimo:

a) Orientação sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE.

b) Descrição do hardware e software de cada equipamento.

c) Configuração e administração dos equipamentos.

d) Descrição geral da plataforma de gerência.

e) Diagnóstico de problemas.

f) Configuração de alarmes, eventos e rotinas para os serviços de monitoramento.

g) Gerência de desempenho e segurança.

h) Manipulação de objetos MIB, SNMP e RMON para monitoração.

i) Resolução de problemas *"troubleshooting"*.

j) Relatórios de acesso.

5.3.5 O programa para a transferência de conhecimento deverá ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

5.3.6 Deverá ser disponibilizado material didático impresso e em formato eletrônico, sem custo adicional para o CONTRATANTE, devendo ainda estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).

5.3.7 Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.

5.3.8 O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissão da Ordem de Serviço na primeira reunião de planejamento.

5.3.9 Caso a transferência de conhecimento não seja satisfatória em relação aos aspectos carga horária, programa apresentado e estrutura de, deverá ser realizado novamente, sem ônus adicional ao CONTRATANTE.

5.3.10 A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos equipamentos e softwares da solução ofertada.

5.4 Quanto ao serviço de garantia da solução

5.4.1 O prazo de garantia dos equipamentos e direito a atualização dos softwares que compõe a solução é de 48 (quarenta e oito) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução.

5.4.2 Os custos relativos ao serviço de garantia dos equipamentos e softwares que compõe a solução já devem estar incluídos no preço dos próprios itens.

5.4.3 O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento dos equipamentos, dos softwares e na integração entre os componentes da solução, mediante a substituição de equipamentos e versões dos softwares ou revisão de configurações, de acordo com as recomendações dos fabricantes, informações presentes nos páginas e manuais de suporte e normas técnicas específicas.

5.4.4 O direito a atualização dos softwares obriga a CONTRATADA a disponibilizar a atualização de bases externas de categorização de sites, mensagens, vírus, malware, assinatura de ataques e vulnerabilidades, bem

como dos demais softwares fornecidos e que compõe a solução, tão logo ocorra o lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.

5.4.5 A reparação de falhas de funcionamento dos componentes da solução deverá ocorrer de acordo com os seguintes princípios:

a) Quanto aos equipamentos da solução:

i. Dispor de estoque de peças e equipamentos de reposição, visando à prestação dos serviços de reparação do funcionamento dos equipamentos durante todo o período de garantia.

ii. Substituir, no prazo de 8 (oito) horas, partes e componentes dos equipamentos que apresentem defeito por outras de características idênticas ou superiores, originais e novas.

iii. Nos casos em que não seja possível o reparo dentro do prazo estipulado acima, substituir no prazo máximo de 72 (setenta e duas) horas, em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso.

iv. Substituir, no prazo de 120 (cento e vinte) horas, qualquer equipamento, componente ou periférico por outro original e novo, na ocorrência dos seguintes casos:

- Se for constatada qualquer divergência com as especificações técnicas descritas na proposta técnica apresentada.
- Se no período de 15 (quinze) dias corridos, contados após a abertura de chamado de Suporte Técnico, ocorrerem defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de partes e componentes.

v. Em todas as hipóteses de substituição previstas anteriormente, caso exista a impossibilidade técnica de substituição por modelo igual, novo e original, será permitida a substituição por outro com características técnicas idênticas ou superiores, plenamente compatível, também original e novo.

vi. Devolver, em perfeito estado de funcionamento, no prazo máximo de 15 (quinze) dias corridos, a contar da data de retirada dos equipamentos, os equipamentos que necessitem ser temporariamente retirados para reparo, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA.

vii. Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidos em função das atividades por estes executadas.

viii. Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos objeto

deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção.

b) Quanto aos softwares da solução:

i. A CONTRATADA deverá promover o isolamento, identificação e caracterização de falhas nos softwares da solução consideradas "*bug de software*".

ii. Será considerado pelo CONTRATANTE como "*bug de software*" o comportamento ou característica dos softwares que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados como prejudiciais ao seu correto uso.

iii. Serão de exclusiva responsabilidade da CONTRATADA o encaminhamento da falha de software ao laboratório do fabricante, o acompanhamento da solução e a aplicação dos respectivo fix, patch ou pacote de correção em dia e horário a ser definido pelo CONTRATANTE.

c) Quanto a integração dos componentes da solução:

i. A CONTRATADA deverá manter, durante a vigência da garantia, a correta integração entre os elementos de hardware e software que compõe a solução, nas mesmas condições de desempenho e confiabilidade que apresentavam no momento de emissão do Termo de Recebimento Definitivo.

ii. Quando forem identificadas falhas de funcionamento na solução que não sejam atribuídas diretamente aos elementos de hardware ou de software, caberá à CONTRADADA a análise e o encaminhamento da solução, buscando restaurar o correto funcionamento do conjunto de elementos da solução.

iii. Serão consideradas como falhas de funcionamento da integração dos componentes a redução significativa do desempenho ou a perda de funcionalidades técnicas disponibilizadas pelo conjunto da solução.

5.4.6 A atualização dos softwares fornecidos que compõe a solução deverá ocorrer de acordo com os seguintes princípios:

a) O CONTRATANTE deverá ter direito irrestrito, durante a vigência da garantia, de atualizar as bases externas de categorização de sites, mensagens, vírus, malware, assinatura de ataques e vulnerabilidades.

b) O CONTRATANTE deverá ter direito irrestrito, durante a vigência da garantia, de atualizar as versões de todos os softwares que compõe a solução, mesmo que os fabricantes alterem suas políticas de licenciamento dos softwares.

c) O direito a atualização de versões dos softwares que compõe a solução não poderá gerar qualquer custo adicional para o CONTRATANTE.

d) Deverão ser criadas contas de acesso, em nome do CONTRATANTE, no sítio internet do fabricante dos softwares que compõe a solução.

e) O perfil das contas criadas em nome do CONTRATANTE deverão permitir de forma irrestrita o download de drivers, firmwares, patches, atualizações, novas versões, informações de suporte, acesso a base de conhecimento e manuais técnicos.

f) Sempre que solicitado mediante chamado de Suporte Técnico, a CONTRATADA deverá orientar o CONTRATANTE quanto aos procedimentos técnicos para a instalação ou atualização de versões dos softwares que compõe a solução.

5.4.7 Juntamente com a documentação de entrega, instalação e configuração da solução, como requisito para a emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

a) Certificado de garantia de que todos os equipamentos que compõe a solução estão cobertos por garantia e suporte técnico on-site, diretamente do fabricante, com prazo de solução de até 8 (oito) horas, pelo período de 48 (quarenta e oito) meses totais exigidos no item 5.4.1.

   i. Caso não seja comercializado item de garantia com o prazo nos moldes exigidos no item anterior, deverá ser entregue pela CONTRATADA declaração oficial, emitida pelo fabricante dos equipamentos, atestando a contratação do serviço de garantia e suporte técnico on-site com o nível de serviço e duração solicitados.

b) Cessões de direito de uso perpétuo dos softwares fornecidos. Os termos de licenciamento de todos os softwares fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão direito pertencentes ao CONTRATANTE.

c) Conjunto de direitos de atualização de versão, pelo período de 48 meses de garantia, de todos os softwares fornecidos. Abrangerá todos os softwares e licenças a serem fornecidos na solução. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e comporão direito pertencente ao patrimônio do CONTRATANTE.

5.5 Quanto ao serviço de suporte técnico

5.5.1 O serviço de suporte técnico on-site para os equipamentos e softwares que compõe a solução deverá ser executado pela CONTRATADA ou diretamente pelo fabricante, durante o prazo de 48 (quarenta e oito) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução.

5.5.2 O serviço de suporte técnico da solução consiste em:

a) Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visando à solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução (equipamentos e softwares), permitindo o retorno à condição normal de operação.

b) Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou outro recursos de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução.

c) Realizar visitas técnicas preventivas no local de instalação da solução (on-site), com frequência mensal, e com duração de pelo menos 8 (oito) horas a cada visita, visando assegurar o melhor desempenho da solução.

d) Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas.

5.5.3 Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, os chamados deverão ser categorizados em 4 (quatro) níveis, da seguinte forma:

Criticidade	**Descrição**	**Prazo máximo para início de atendimento (contados a partir da abertura do chamado)**	**Prazo máximo para restauração de serviço (contados a partir da abertura do chamado)**
Severidade 1 (Alta)	Atuação ON-SITE visando sanar problemas que tornem a solução integrada de segurança inoperante, causando alto impacto nas operações de TI do CJF.	Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 6 (seis) horas
Severidade 2 (Média/Alta)	Atuação ON-SITE visando sanar problemas que prejudicam a operação normal da solução, mas não interrompem o acesso aos sistemas de TI, causando impacto no ambiente de produção ou restrição de funcionalidade.	Em até 4 (quatro) horas deve ter um técnico da COTRATADA ON-SITE.	Em até 12 (doze) horas
Severidade 3 (Média/Baixa)	Atuação REMOTA visando sanar problemas ou dúvidas que criem restrições a operação normal da solução integrada de segurança não gerando impacto ao negócio.	Em até 4 (quatro) horas um técnico da CONTRATADA entra em contato.	Em até 24 (vinte e quatro) horas
Severidade 4 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução integrada de segurança, ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 72 (setenta e duas) horas

5.5.4 O CONTRATANTE realizará a abertura de chamados técnicos de suporte por meio de ligação telefônica ou via Internet, em período integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

5.5.5 A CONTRATADA deverá informar o procedimento para abertura de chamado técnico de suporte no documento plano de implantação.

5.5.6 Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

5.5.7 Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar o número do chamado, para fins de controle.

5.5.8 A CONTRATADA deverá enviar mensalmente, ou disponibilizar acesso por meio de portal internet, relação consolidada dos chamados abertos no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, problemas verificados, técnico responsável pelo atendimento.

5.5.9 A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.

5.5.10 A CONTRATADA deverá realizar a cada ocorrência, como escopo das atividades de visitas técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos equipamentos e softwares que compõe a solução integrada de segurança, buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas à solução.

5.5.11 As visitas técnicas preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s) nas áreas de gerenciamento de ameaças, análise de vulnerabilidades e firewall de aplicação, devendo possuir certificação emitida pelos fabricantes dos equipamentos e softwares da solução ofertada. As visitas técnicas serão prestadas com acompanhamento da equipe técnica do CJF.

5.5.12 A contagem de prazo para a realização das visitas técnicas preventivas será iniciado após emissão do Termo de Recebimento Definitivo da solução, devendo ocorrer automaticamente em dia e hora previamente agendada com o CJF e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CJF. A cada visita deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho, aplicação de funcionalidade e revisão dos aspectos de segurança.

5.5.13 A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CJF, em

relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

6 (...)

7 (...)

8 (..)

9 (...)

10 (...)

11 MODELO DE REMUNERAÇÃO (Glosas)

11.1 O não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico por ocorrência, independentemente das Sanções Administrativas previstas no Contrato, implicará em redutor na fatura mensal do serviço de suporte técnico (glosa), nos seguintes casos:

11.1.1 Glosa de 5% (cinco por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade alta**, limitada até 06 (seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

11.1.2 Glosa de 3% (três por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade média/alta**, limitada até 12 (doze) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

11.1.3 Glosa de 2% (dois por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade média/baixa**, limitada até 18 (dezoito) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

11.1.4 Glosa de 1% (dois por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade baixa**, limitada até 36 (trinta e seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

11.1.5 Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas previstas, a cada ocorrência a CONTRATADA receberá uma Sanção de Advertência, a ser aplicada pela área Administrativa do CONTRATANTE.

11.2 A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços.

11.3 O faturamento do serviço de suporte técnico deverá ser mensal, mediante apresentação de nota de cobrança consolidada para todos os equipamentos e softwares da solução, já descontadas as glosas eventualmente aplicadas em função

do não atendimento dos níveis de qualidade definidos no contrato, determinando o valor total do serviço para o mês.

11.4 No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses, serão aplicadas as Sanções Administrativas previstas no Contrato.

11.5 No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa.

11.6 Se a decisão da Administração for favorável ao recurso da CONTRATADA, a mesma emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

11.7 A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

12 (...)

13 CONFIDENCIALIDADE

13.1 A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações relativas à:

i) Política de segurança adotada pelo CJF e configurações de hardware e software decorrentes.

ii) Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos em atendimento aos itens de segurança constantes do(s) objeto(s) instalado(s).

13.2 A CONTRATADA deverá concordar e assinar Termo de Confidencialidade e Sigilo da Contratada (ANEXO V), entregando o Termo assinado pelo representante legal da empresa, com firma reconhecida.

14 (...)

15 (...)

16 (...)

17 (...)

18 DOCUMENTOS ANEXOS

Seguem anexos a este Termo de Referência os seguintes documentos:

a) Anexo I – Especificação Técnica da Solução.

b) Anexo II – Ambiente Tecnológico do CJF.

c) Anexo III – Cronograma de Implantação.

d) Anexo IV – Termo de Confidencialidade e Sigilo da Licitante.

e) Anexo V – Termo de Confidencialidade e Sigilo da Contratada.

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

A solução integrada de segurança a ser fornecida deverá ser integrada a estrutura tecnológica em uso no CJF composta por switches core, servidores, switches topo de rack, de acordo com os modelos e versões detalhadas no documento **Ambiente Tecnológico do CJF (ANEXO II)**. Será de responsabilidade da empresa CONTRATADA o fornecimento e instalação de todos os itens acessórios de hardware e software necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, adaptadores, suportes, drivers de controle, programas de configuração, cordões ópticos e demais componentes necessários para a perfeita integração da solução a infraestrutura existente no CONTRATANTE.

São apresentadas, a seguir, especificações técnicas mínimas dos equipamentos a serem ofertados referentes aos subitens 1.1, 1.2 e 1.3 do objeto. Os verbos “possuir”, “permitir”, “suportar” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

Todos os componentes necessários à solução deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do CONTRATANTE.

Os componentes da solução integrada de segurança deverão ocupar no máximo 20U (Vinte Rack Units) de espaço no rack, considerando o somatório dos espaços utilizados por todos os componentes da solução (Itens 1.1, 1.2 e 1.3).

ITEM 1.1 - SOLUÇÃO DE GERENCIAMENTO DE AMEAÇAS

Os equipamentos, produtos, peças ou softwares necessários à Solução de Gerenciamento de Ameaças deverão ser instalados no *datacenter* do CONTRATANTE, devendo observar os seguintes requisitos mínimos:

1.1.1. Ser provido com emprego de, no mínimo, 2 (dois) elementos para serem fixados em *rack* padrão 19”, sendo que o conjunto dos requisitos especificados poderá ser atendido por meio de outros equipamentos.

1.1.2. Permitir alta disponibilidade com tolerância a falhas, sendo admitida apenas a configuração ativo-ativo.

1.1.3. Possuir fontes de alimentação 220v, redundantes N+1.

1.1.4. Suportar toda a pilha IPv4/IPv6.

1.1.5. Permitir a aplicação de novas políticas em tempo real, sem interrupção do tráfego.

1.1.6. Na função de firewall de rede:

1.1.6.1. Proteger 3 (três) segmentos de rede físicos, utilizando 1 (uma) porta de comunicação dedicada 10GbE (10 Gigabit Ethernet) para cada um dos segmentos.

1.1.6.2. Possuir pelo menos 8 (oito) portas de comunicação dedicada, padrão Gigabit Ethernet (Cobre ou 1000Base-T SFP).

1.1.6.3. Deverão ser fornecidos os respectivos transceivers SFP+ 10GBASE-SR, SFP, licenças de uso das portas e cordões óticos duplex MMF LC/LC, com comprimento máximo de 10m, necessários para a interligação das portas externas ao switch core do Datacenter.

1.1.6.4. Possuir porta independente para gerência, padrão Gigabit Ethernet (Cobre

ou 1000base-T SFP ou 1000base-SX Conector LC) ou superior.

1.1.6.5. Possuir porta(s) independente(s) para sincronismo de cluster, padrão Gigabit Ethernet (Cobre ou 1000base-T SFP ou 1000base-SX Conector LC) ou superior.

1.1.6.6. Deverão ser fornecidos 20 (vinte) patch cords CAT. 6 certificados, com comprimento de pelo menos 5 (cinco) metros, necessários a interligação das portas externas ao switch core do Datacenter.

1.1.6.7. Possuir throughput de firewall de 30 (trinta) Gbps.

1.1.6.8. Permitir tratar 1.000.000 (hum milhão) de sessões simultâneas.

1.1.6.9. Permitir a admissão 100.000 (cem mil) novas conexões por segundo.

1.1.6.10. Permitir no mínimo 1024 (hum mil e vinte e quatro) regras de firewall.

1.1.6.11. Permitir o estabelecimento de túneis IPSec com VPN com throughput de no mínimo 1 (um) Gbps de tráfego para criptografia usando 3DES.

1.1.6.12. Permitir a filtragem de pacotes baseada em estados (stateful inspection).

1.1.6.13. Permitir o registro dos fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas os endereços de origem e destino dos pacotes, portas TCP e UDP de origem e destino, bem como números de sequência de pacotes TCP.

1.1.6.14. Suportar toda a pilha de protocolos do modelo TCP/IP, com as seguintes funcionalidades:

1.1.6.14.1. Fazer inspeção stateful de tráfego.

1.1.6.14.2. Suportar roteamento estático de tráfego.

1.1.6.15. Permitir o funcionamento em modo transparente tipo bridge e permitir ser configurado em alta disponibilidade neste modo.

1.1.6.16. Permitir a criação de regras por endereço de origem e destino, sub-rede IP, protocolo de rede, porta de destino e tipo de serviço. Também deverá permitir a identificação da interface de rede de origem, quando a tecnologia do equipamento permitir.

1.1.6.17. Permitir a definição de período de validade de regras, ou seja, determinar a validade de uma regra de acordo com o horário, data ou dia da semana.

1.1.6.18. Permitir o uso de NAT (Network Address Translation) e PAT (Protocol Address Translation).

1.1.6.19. Suportar tags de VLAN trunking (802.1q), sendo possível configurar pelo menos 255 (duzentas e cinqüenta e cinco) vlan-id em uma mesma interface física.

1.1.6.20. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.

1.1.6.21. Permitir sincronização do relógio utilizando o protocolo NTP ou SNTP para sincronizar com bases externas.

1.1.6.22. Permitir proteção contra ataques de:

1.1.6.22.1. SYN Flood.

1.1.6.22.2. IP Spoofing.

1.1.6.22.3. UDP Flood.

1.1.6.23. Suportar os protocolos de roteamento BGP4 e OSPF v.2.

1.1.6.24. Possuir funcionalidade de servidor DHCP e Relay DHCP.

1.1.6.25. Permitir o estabelecimento de túneis (VPN site-to-site) com, no mínimo as seguintes especificações:

1.1.6.25.1. Utilizar protocolo IPSEC e IPSEC NAT traversal.

1.1.6.25.2. Efetuar troca de chaves por meio de protocolo IKE e certificados X. 509.

1.1.6.25.3. Criptografar utilizando especificação AES (256 bits).

1.1.6.25.4. Permitir a utilização de pelo menos 512 túneis simultâneos.

1.1.6.26. Permitir a criação dinâmica a partir da análise da sinalização H.225 e H.245 (Call Setup e Call Control, respectivamente) de regras pertinentes para tráfego de mídia (RTP/RTCP) entre as MCUs do CJF e as estações de videoconferência da Justiça Federal, consistindo tais regras em combinações de:

1.1.6.26.1. IP e porta de origem (elemento originador da chamada).

1.1.6.26.2. IP e porta de destino (elemento recipiente da chamada).

1.1.6.26.3. Interfaces de entrada e saída do tráfego de vídeo com inspeção stateful.

1.1.6.27. Suportar as versões 2, 3 e 4 do Framework H.323.

1.1.6.28. Suportar Multicast.

1.1.6.29. Permitir a administração por ferramenta com interface gráfica remota segura, utilizando browser.

1.1.6.30. Permitir a administração por interface de linha de comando (CLI – Command Line Interface) com uso de protocolo de comunicação SSH-2.

1.1.6.31. Permitir a replicação de configurações e a aplicação de atualização de software para os elementos dos nós do cluster.

1.1.6.32. Permitir a definição de diferentes níveis de administração, sendo ao menos um nível completo e outro somente de visualização de configurações e logs.

1.1.6.33. Caso a solução de gestão de ameaças exija servidor físico de uso genérico para a execução de qualquer de suas funcionalidades, o equipamento ofertado deverá atender aos seguintes requisitos:

- Servidor tipo rack, para instalação em rack padrão de 19", limitado a 2U de altura.
- Possuir pelo menos 1 (um) processador de 8 (oito) núcleos, arquitetura de 64 bits.
- Possuir pelo menos 32GB de memória RAM DDR3.
- Possuir pelo menos 2 (dois) discos internos com configuração mínima de 300 GB, tecnologia SAS, velocidade de 10.000 RPM.
- Possuir pelo menos 2 (duas) portas GbE 1000Base-T.
- Possui fonte de alimentação 220V, redundantes N+1.

1.1.7. Na função de gerência de qualidade de serviço:

1.1.7.1. Permitir controle e priorização de tráfego, priorizando e garantindo banda para as aplicações através da classificação dos pacotes, criação de filas de prioridade, gerencia de congestionamento e QoS.

1.1.7.2. Permitir modificação de valores DSCP para o Diffserv.

1.1.7.3. Limitar individualmente a banda utilizada por diferentes aplicações e serviços tanto para tráfego entrante a internet quanto sainte.

1.1.8. Na função de filtro de conteúdo:

1.1.8.1. Suportar throughtput de, no mínimo, 1 (um) Gbps de tráfego.

1.1.8.2. Suportar no mínimo 800 usuários simultâneos.

1.1.8.3. Permitir a utilização de pelo menos 40 (quarenta) categorias para classificação de sites web.

1.1.8.4. Possuir base mínima contendo ao menos 20 (vinte) milhões de sites internet web já registrados e classificados, pelo menos nos idiomas inglês, português e espanhol.

1.1.8.5. Permitir atualização automática de base de URLs via internet com base do fabricante durante todo o período contratual.

1.1.8.6. Possuir categoria exclusiva no mínimo para os seguintes tipos de sites web:

1.1.8.6.1. Compras.

1.1.8.6.2. Hacker.

1.1.8.6.3. Instituições governamentais.

1.1.8.6.4. Notícias.

1.1.8.6.5. Phishing.

1.1.8.6.6. Pornografia.

1.1.8.6.7. Proxy.

1.1.8.6.8. Racismo.

1.1.8.6.9. Redes sociais.

1.1.8.6.10. Webmail.

1.1.8.7. Permitir a recategorização de sites, diferente da categorização original do site.

1.1.8.8. Permitir monitoração do tráfego interno sem bloqueio de acesso aos usuários.

1.1.8.9. Permitir identificação dos usuários de maneira integrada com LDAP e Active Directory para aplicação de políticas de controle, priorização e filtragem de tráfego WEB.

1.1.8.10. Permitir integração com grupos ou OUs (Organizational Units) no Active Directory.

1.1.8.11. Permitir identificação transparente de usuários cadastrados no Active Directory, sem necessidade de entrada de usuário e senha para usuários já logados em estação de trabalho utilizando Windows XP/Windows 7.

1.1.8.12. Permitir customização de mensagens para resposta aos usuários.

1.1.8.13. Permitir a filtragem de conteúdo WEB de códigos (programas/scripts) maliciosos.

1.1.8.14. Permitir a atualização regular do produto e suas bases de dados sem interromper a execução dos serviços de filtragem.

1.1.8.15. Suportar Proxy do tráfego WEB a ser filtrado no mínimo nos protocolos HTTP e HTTPS.

1.1.8.16. Permitir a operação como Proxy explícito e transparente, de acordo com a interface.

1.1.8.17. Permitir filtragem de tráfego criptografado via SSL tanto na entrada como na saída, atuando como interceptor de tráfego (man-in-the-middle).

1.1.8.18. Suportar a verificação de certificados de URL solicitadas, permitindo bloqueio caso o certificado seja classificado como inválido.

1.1.8.19. Permitir filtros de URL customizados por políticas.

1.1.8.20. Permitir filtros de URL baseado em base de dados local.

1.1.8.21. Suportar o bloqueio de requisições por meio de filtros de extensão de arquivos.

1.1.8.22. Permitir controle de acesso a sites HTTP/HTTPS por meio de lista negra e lista branca armazenada localmente.

1.1.8.23. Permitir ou bloquear sites ou categorias de sites:

1.1.8.23.1. Por grupo do Active Directory.

1.1.8.23.2. Por Organization Unit (OU) do Active Directory.

1.1.8.23.3. Por faixa de tempo.

1.1.8.23.4. Por expressões de requisição URL.

1.1.8.23.5. Por domínio de URL.

1.1.8.24. Permitir o uso de expressões regulares para filtrar conteúdo existente no cabeçalho HTTP.

1.1.8.25. Suportar o controle de aplicações que trafeguem dados pela internet, permitindo monitoração e bloqueio das mesmas.

1.1.8.26. Suportar regras de exceção a tráfego SSL que não deve ser inspecionado.

1.1.8.27. Suportar integração com solução de antivírus de gateway por meio do protocolo ICAP ou possuir a solução de antivírus incorporada no produto.

1.1.8.28. Suportar inspeção de conteúdo para verificação e eliminação de vírus e malwares.

1.1.8.29. Permitir a detecção de conteúdos maliciosos, suspeitos ou de atividades indesejadas por meio de análise comportamental do código, proporcionando proteção contra ameaças desconhecidas (Proteção Dia Zero).

1.1.8.30. Suportar análise de objetos encapsulados com a opção de bloqueio.

1.1.8.31. Suportar verificações de malware de forma concorrente para cada objeto analisado, em tempo real.

1.1.8.32. Verificar tráfego analisando os dados até a camada 7 do modelo OSI, identificando estações de trabalho da rede interna possivelmente

infectadas por malwares.

1.1.8.33. Permitir identificar e bloquear aplicações maliciosas, inclusive dos tipos:

1.1.8.34. *ActiveX*.

1.1.8.35. Executáveis *Windows*.

1.1.8.36. *Flash ActionScripts*.

1.1.8.37. *Java applets*.

1.1.8.38. *Java applications*.

1.1.8.39. *Java Scripts*.

1.1.8.40. potencialmente não desejados (*spywares*).

1.1.8.41. *Visual Basic*.

1.1.8.42. Permitir bloquear todos os comportamentos/técnicas abaixo:

1.1.8.42.1. Data theft: Backdoor.

1.1.8.42.2. Data theft: Keylogger.

1.1.8.42.3. Data theft: Password stealer.

1.1.8.42.4. Data theft: Spyware.

1.1.8.42.5. Detection evasion: Obfuscated code.

1.1.8.42.6. Detection evasion: Packed code.

1.1.8.42.7. Phishing (para webmail).

1.1.8.42.8. Potentially unwanted: Ad-/Spyware.

1.1.8.42.9. Potentially unwanted: Adware.

1.1.8.42.10. Potentially unwanted: Deceptive behavior.

1.1.8.42.11. Potentially unwanted: Dialer.

1.1.8.42.12. Potentially unwanted: Privacy violation.

1.1.8.42.13. Potentially unwanted: Redirector.

1.1.8.42.14. Potentially unwanted: Suspicious activity.

1.1.8.42.15. Stealth activity: Code injection.

1.1.8.42.16. Stealth activity: Rootkit.

1.1.8.42.17. System compromise: Browser exploit.

1.1.8.42.18. System compromise: Code execution exploit.

1.1.8.42.19. System compromise: Trojan downloader.

1.1.8.42.20. System compromise: Trojan dropper.

1.1.8.42.21. System compromise: Trojan proxy.

1.1.8.42.22. System compromise: Trojan.

1.1.8.42.23. Viral Replication: File infector vírus.

1.1.8.42.24. Viral Replication: Network worm.

1.1.8.42.25. Web threats: Cross-site scripting.

1.1.8.42.26. Web threats: Infected website.

1.1.8.42.27. Web threats: Vulnerable ActiveX controls.

1.1.9. Na função de balanceamento de carga:

1.1.9.1. Permitir o balanceamento de no mínimo 5 servidores reais para um servidor virtual, de forma transparente aos usuários finais.

1.1.9.2. Permitir o uso dos seguintes métodos de balanceamento:

1.1.9.2.1. Estático.

1.1.9.2.2. Round-robin.

1.1.9.2.3. Baseado na disponibilidade do servidor real.

1.1.9.2.4. Baseado no número de conexões.

1.1.9.2.5. Baseado no menor round trip time.

1.1.9.3. Permitir o balanceamento de HTTP, HTTPS e SSL.

1.1.9.4. Permitir o balanceamento de serviços genéricos em camada 4 (TCP e UDP).

1.1.9.5. Permitir o balanceamento de protocolos IP genéricos em camada 3.

1.1.9.6. Permitir o balanceamento de tráfego entre dois links internet de duas operadoras distintas, realizando a monitoração da disponibilidade de cada link e, em caso de detecção de queda de um dos links internet, deve direcionar o tráfego para o outro link. Quando o link que falhou for restabelecido, deverá retomar o balanceamento pelos dois links.

1.1.10. Na função de antivírus de Gateway:

1.1.10.1. Permite a inspeção de tráfego em tempo real por vírus nos protocolos HTTP, SMTP e FTP.

1.1.10.2. Permite o bloqueio de download de arquivos por tipo.

1.1.10.3. Permite o bloqueio de download de arquivos maliciosos do tipo adware, spyware, hijackers, keyloggers, etc.

1.1.11. Na função de prevenção de intrusão:

1.1.11.1. Permitir a utilização de IPS inline protegendo no mínimo o mesmo número de interfaces definidas no item 1.1.6.1.

1.1.11.2. Permite a detecção e proteção contra intrusão de hosts/redes.

1.1.11.3. Possuir a capacidade de remontar pacotes para identificação de ataques.

1.1.11.4. Suportar contenção de pelo menos os seguintes mecanismos de detecção e proteção de ataques:

1.1.11.4.1. Análise de protocolos.

1.1.11.4.2. Detecção de anomalias.

1.1.11.4.3. Detecção de ataques de RPC e MS-RPC.

1.1.11.4.4. Reconhecimento de padrões.

1.1.11.4.5. Proteção/bloqueio contra ataques nos protocolos SMB v1, v2 e v2.1, SMTP, IMAP, POP, DNS, SYSLOG, SSL, FTP, SSH, ICMP, HTTP/HTTPS, PEER-2-PEER, H.225 e SIP.

1.1.11.5. Possuir ao menos os seguintes métodos de notificação:

1.1.11.5.1. Registro na console de administração.

1.1.11.5.2. Alertas via correio eletrônico ou trap SNMP.

1.1.11.6. Possuir ao menos os seguintes métodos de resposta a ataques:

1.1.11.6.1. Armazenamento de log de sessão.

1.1.11.6.2. Inclusão de host/rede em lista negra.

1.1.11.6.3. Termino de sessões via reset de conexão TCP.

1.1.11.7. Permitir atualização automática das assinaturas para o sistema de detecção de intrusão.

1.1.11.8. Permitir a mitigação de efeitos de ataque de negação de serviço.

1.1.11.9. Permitir a filtragem de ataque por anomalia de tráfego.

1.1.11.10. Permitir filtragem de ataque de negação de serviço, reconhecimento, exploit e evasão de firewall.

1.1.11.11. Permitir filtragem de ataque na camada de aplicação.

1.1.11.12. Permitir throughput de inspeção de tráfego de no mínimo 6 (seis) GBps (Gigabits por segundo).

1.1.11.13. Permitir implantação de identificação de intrusão (passivo) ou prevenção de intrusão (ativo) simultaneamente no mesmo equipamento, em regras para pares de redes ou hosts diferentes, mesmo as regras sejam aplicáveis as mesmas interfaces.

1.1.11.14. Permite inspeção utilizando técnicas de inspeção profunda de pacotes (DPI – Deep Packet Inspection) ou na modalidade Stateful Inspection.

1.1.11.15. Permite a detecção e prevenção de ataques não orientados à conexão.

1.1.11.16. Permite a execução de todas as funções de inspeção sem a instalação de agentes nos hosts a serem protegidos.

1.1.12. Deverá ser fornecidos manuais de operação e configuração do(s) equipamento(s) proposto(s) em português ou inglês (cabos, acessórios e programas de configuração necessários à completa operacionalização dos recursos exigidos nesta especificação.

ITEM 1.2 - SOLUÇÃO DE GESTÃO DE VULNERABILIDADES

Os equipamentos, produtos, peças ou softwares necessários à Solução de Gerenciamento de Ameaças deverão ser instalados no *datacenter* do CONTRATANTE, devendo observar os seguintes requisitos mínimos:

1.2.1 Deverá ser provida com emprego de 1 (um) elemento com função de gestão de vulnerabilidades, para ser fixado em rack padrão 19", ou como funcionalidade junto do **ITEM 1.1**.

1.2.2 Serão aceitas soluções em forma de "*appliance*", porém caso a solução de gestão de vulnerabilidades exija servidor físico de uso genérico para sua instalação, o equipamento ofertado deverá atender aos seguintes requisitos:

- Servidor tipo rack, para instalação em rack padrão de 19", limitado a 2U de altura.
- Possuir pelo menos 1 (um) processador de 8 (oito) núcleos, arquitetura de 64 bits.
- Possuir pelo menos 32GB de memória RAM DDR3.
- Possuir pelo menos 2 (dois) discos internos com configuração mínima de 300 GB, tecnologia SAS, velocidade de 10.000 RPM.
- Possuir pelo menos 2 (duas) portas GbE 1000Base-T.
- Possui fonte de alimentação 220V, redundantes N+1.

1.2.3 Os componentes da solução integrada de segurança deverão ocupar no máximo 20U (Vinte Rack Units) de espaço no rack, considerando o somatório dos espaços utilizados por todos os componentes da solução.

1.2.4 Permitir efetuar descoberta de topologia dos ativos da rede (qualquer servidor ou ativo de rede que possua endereço IP ou que seja alocado no escopo desta contratação).

1.2.5 Permitir a integração visando a atualização automática da tabela de ativos do CONTRATANTE (CMDB), baseada na ferramenta CA Service Desk, das informações sobre os serviços e as vulnerabilidades encontradas no ativo analisado.

1.2.6 Permitir correlacionar eventos baseados nos sistema operacional, Porta/Protocolo, Banners e vulnerabilidades.

1.2.7 Permitir detectar vulnerabilidades em aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede.

1.2.8 Permitir verificar vulnerabilidades em ambiente Windows para, no mínimo: detecção de hot fixes, service packs, registros, backdoors, trojans, malwares, peer to peer, portas de serviço habilitadas e antivírus.

1.2.9 Suportar efetuar varredura à procura de vulnerabilidades e exploits.

1.2.10 Permitir detectar vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede.

1.2.11 Permitir a descoberta das vulnerabilidades para os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço e para todo o ambiente computacional do CJF escopo deste projeto, nas quantidade e versões especificados nos Subitens 2 e 3 do ANEXO II.

1.2.12 Para executar a análise de vulnerabilidades, deverá permitir:

1.2.12.1 Utilizar listas de vulnerabilidades da SANS/FBI e IAVA (Information Assurance Vulnerability Alert) ou possuir catalogado em suas bases mais de 50 (cinqüenta) mil vulnerabilidades.

1.2.12.2 Integrar-se com base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures) .

1.2.12.3 Possuir módulos de varredura diferenciados para análise intrusiva e não intrusiva.

1.2.12.4 Analisar aplicações web para detecção de vulnerabilidades, tais como Cross-Site-Scripting.

1.2.12.5 Efetuar varredura por endereço IP, Sistema Operacional, nome DNS, nome NetBIOS ou nome do domínio.

1.2.13 Deve permitir a filtrar a varredura por:

1.2.13.1 Destino.

1.2.13.2 Serviço.

1.2.13.3 Vulnerabilidade.

1.2.14 Suportar mecanismos para varredura de vulnerabilidades de hosts, bancos de dados e aplicações web, incluindo a detecção de vulnerabilidades em AJAX e WEB 2.0.

1.2.15 Suportar a verificação de vulnerabilidades:

1.2.15.1 De forma não invasiva.

1.2.15.2 Por tipo de risco.

1.2.15.3 Categoria.

1.2.15.4 Por correlação de bases CVE.

1.2.16 Suportar análise de aplicação WEB a procura de informações em comentários HTML, hyperlinks, endereços de correio, keywords, campos escondidos e scripts.

1.2.17 Permitir identificar vulnerabilidades em queries SQL de aplicações WEB, suscetíveis a SQL injection.

1.2.18 Permitir analisar esquema de autenticação WEB.

1.2.19 Suportar pontuação que permite medir o nível de risco dos sistemas e dos recursos de rede CJF.

1.2.20 Permitir levantamento e classificação quanto à criticidade de todos os ativos protegidos.

1.2.21 Permitir a apresentação do nível de criticidade de cada ativo, indicando seu grau de exposição a worms, exploits e malwares em geral.

1.2.22 Possuir capacidade de configurar a velocidade da varredura de forma a não impactar a desempenho da rede.

1.2.23 Permitir a geração de alertas com informações detalhadas sobre o nome da vulnerabilidade, descrição detalhada, hosts afetados incluindo endereço IP e nome comum, os serviços abertos no host e as vulnerabilidades afetadas.

1.2.24 Informar e avaliar periodicamente a vulnerabilidade do Conselho a eventuais falhas de segurança dos componentes de seu ambiente de TI, com o objetivo de indicar atualizações ou procedimentos necessários para eliminar ou mitigar as Vulnerabilidades.

1.2.25 Disponibiliza relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição dos ativos do CJF aos riscos identificados com, pelo menos, as seguintes informações:

1.2.25.1. Hosts descobertos.

1.2.25.2. Nível de risco por plataforma e por vulnerabilidade.

1.2.25.3. Score com o nível de risco.

1.2.25.4. Serviços descobertos.

1.2.25.5. Sumário.

1.2.25.6. Topologia de rede descoberta.

1.2.25.7. Vulnerabilidades em aplicações WEB.

1.2.25.8. Vulnerabilidades em Windows.

1.2.25.9. Vulnerabilidades encontradas.

1.2.26 Executar auditorias do ambiente utilizando os dados coletados e registrados na base de dados.

1.2.27 Permitir o gerenciamento de baselines de configuração dos ativos, que podem ser comparados com as novas avaliações para a determinação de desvios e envia alertas por e-mail.

1.2.28 Suportar verificação de configurações e permissões nas plataformas de sistemas operacionais e bases de dados, para:

1.2.28.1. Linux RED HAT.

1.2.28.2. Linux SUSE.

1.2.28.3. Oracle.

1.2.28.4. SQL Server.

1.2.28.5. Windows.

1.2.29 Possuir ferramenta de administração com interface gráfica remota segura, a partir de plataforma Windows 7, Windows XP ou interface WEB, e permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs.

ITEM 1.3 – SOLUÇÃO DE FIREWALL DE APLICAÇÃO

Os equipamentos, produtos, peças ou softwares necessários à Solução de Firewall de Aplicação deverão ser instalados no *datacenter* do CONTRATANTE, devendo observar os seguintes requisitos mínimos:

1.3.1. Deverá ser provida com emprego de 2 (dois) elementos com função de firewall de aplicação (WAF), para serem fixados em rack padrão 19", ou como funcionalidade junto do **ITEM 1.1**.

1.3.2. Os componentes da solução integrada de segurança deverão ocupar no máximo 20U (Vinte Rack Units) de espaço no rack, considerando o somatório dos espaços utilizados por todos os componentes da solução.

1.3.3. Implementar cluster de alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo.

1.3.4. Possuir fontes de alimentação 220v, redundantes N+1.

1.3.5. Cada um dos nós do cluster deve:

1.3.5.1. Proteger 3 (três) segmentos de rede físicos utilizando 2 (duas) portas de comunicação, dedicada Gigabit Ethernet (Cobre ou 1000Base-T SFP ou 1000Base-SX conector LC) para cada um dos segmentos.

1.3.5.2. Deverão ser fornecidos 20 (vinte) patch cords CAT. 6 certificados, com comprimento de pelo menos 5 (cinco) metros, necessários a interligação das portas externas ao switch core do Datacenter.

1.3.5.3. Possuir porta independente para gerência, padrão Gigabit Ethernet (Cobre ou 1000Base-T SFP ou 1000Base-SX conector LC).

1.3.5.4. Possuir porta(s) independente(s) para sincronismo de cluster, padrão Gigabit Ethernet (Cobre ou 1000Base-T SFP ou 1000Base-SX conector LC).

1.3.5.5. Inspecionar 1 (um) Gbps de tráfego de application firewall.

1.3.5.6. Admitir 35.000 (trinta e cinco mil) novas conexões por segundo (transações por segundo – TPS) para cada nó de cluster.

1.3.5.7. Suportar agregação de portas (trunk).

1.3.5.8. Suportar o protocolo 802.1q.

1.3.5.9. Analisar tráfego HTTP/0.9, HTTP/1.0 e HTTP/1.1.

1.3.5.10. Restringir métodos HTTP/HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.

1.3.5.11. Permitir as seguintes opções de implementação:

1.3.5.11.1. Monitoramento (sniffing).

1.3.5.11.2. Proxy (reverso e transparente).

1.3.5.12. permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento.

1.3.5.13. remover as mensagens de erro do conteúdo que será enviado aos usuários.

1.3.5.14. em modo “monitoramento” (sniffing), realiza análise e avaliação do tráfego, gera relatórios com os dados analisados e simula bloqueios para efeito de avaliação.

1.3.5.15. proteger contra ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos.

1.3.5.16. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:

1.3.5.16.1. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações.

1.3.5.16.2. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS.

1.3.5.16.3. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra ataques conhecidos aos protocolos HTTP e HTTPS.

1.3.5.16.4. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão.

1.3.5.16.5. Bloqueio com intermediação e interrupção da conexão.

1.3.5.16.6. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações.

1.3.5.16.7. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios.

1.3.5.16.8. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação.

1.3.5.17. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de

aplicação.

1.3.5.18. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

1.3.5.18.1. Cópia da tentativa do ataque.

1.3.5.18.2. Endereços IP que originaram os ataques.

1.3.5.18.3. Horário do ataque.

1.3.5.18.4. Nome do ataque.

1.3.5.18.5. Qual campo foi atacado.

1.3.5.18.6. Quantas vezes esse ataque foi realizado.

1.3.5.19. Armazenar informações de identificação dos usuários autenticados nas aplicações.

1.3.5.20. Suportar request compression e response compression.

1.3.5.21. Assinar cookies digitalmente e edita endereços de URL ("URL Rewriting").

1.3.5.22. Proteger as aplicações de banco de dados contra ataques conhecidos.

1.3.5.23. Suportar aplicações que utilizam autenticação com estes métodos:

1.3.5.23.1. Autenticação básica.

1.3.5.23.2. NTLM.

1.3.5.23.3. Certificados SSL.

1.3.5.24. Possuir a capacidade de importar os certificados e pares de chaves pública/privada para as soluções que utilizam SSL para transferência de dados, atuando como *man-in-the-middle* para tráfego SSL.

1.3.5.25. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório e ainda se é somente-leitura), cookies, arquivos XML, ações SOAP, e elementos XML.

1.3.5.26. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP.

1.3.5.27. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.

1.3.5.28. Correlaciona múltiplos eventos de segurança em conjunto para distinguir de forma precisa o tráfego permitido do tráfego malicioso.

1.3.5.29. Identifica ataques baseados em:

1.3.5.29.1. Assinaturas, com atualização diária da base pelo fabricante.

1.3.5.29.2. Regras.

1.3.5.29.3. Perfis de utilização.

1.3.5.30. Detectar ataques de força bruta por meio dos seguintes métodos:

1.3.5.30.1. Aumento do tempo de resposta da aplicação monitorada.

1.3.5.30.2. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.

1.3.5.31. Detectar ataques do tipo força bruta em que:

1.3.5.31.1. O atacante solicita repetidamente o mesmo recurso.

1.3.5.31.2. O atacante realiza repetidas tentativas não autorizadas de acesso.

1.3.5.31.3. São utilizados ataques automatizados de login.

1.3.5.32. Detectar ataques do tipo força bruta que explorem:

1.3.5.32.1. Controles de acesso da aplicação (Erro 401 – Unauthorized).

1.3.5.32.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação.

1.3.5.32.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação).

1.3.5.32.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de IPs).

1.3.5.32.5. Clientes automatizados (robôs, requisições muito rápidas).

1.3.5.33. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.

1.3.5.34. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento.

1.3.5.35. Filtra e valida funções XML específicas da aplicação.

1.3.5.36. Possibilitar atualização de novas assinaturas para ataques conhecidos.

1.3.5.37. Apresentar proteção positiva e segura contra ataques, como:

1.3.5.37.1. Anonymous Proxy Vulnerabilities.

1.3.5.37.2. Brute Force Login.

1.3.5.37.3. Buffer Overflow.

1.3.5.37.4. Cookie Injection.

1.3.5.37.5. Cookie Poisoning.

1.3.5.37.6. Cross Site Request Forgery (CSRF).

1.3.5.37.7. Cross Site Scripting (XSS).

1.3.5.37.8. Directory Traversal.

1.3.5.37.9. Forceful Browsing.

1.3.5.37.10. Form Field Tampering.

1.3.5.37.11. HTTP Denial of Service.

1.3.5.37.12. HTTP hidden field manipulation.

1.3.5.37.13. HTTP parameter pollution.

1.3.5.37.14. HTTP request smuggling.

1.3.5.37.15. HTTP Response Splitting.

1.3.5.37.16. HTTP Verb Tampering.

1.3.5.37.17. Illegal Encoding.

1.3.5.37.18. Known Worms.

1.3.5.37.19. LDAP injection.

1.3.5.37.20. Malicious Encoding.

1.3.5.37.21. Malicious Robots.

1.3.5.37.22. Parameter Tampering.

1.3.5.37.23. Remote File Inclusion Attacks.

1.3.5.37.24. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI).

1.3.5.37.25. Session Hijacking.

1.3.5.37.26. Site Reconnaissance.

1.3.5.37.27. SQL Injection.

1.3.5.37.28. Web Scraping.

1.3.5.37.29. Web server software and operating system attacks.

1.3.5.37.30. Web Services (XML) attacks.

1.3.5.37.31. Zero Day Malware.

1.3.5.38. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.

1.3.5.39. Permitir definir regras de tamanho para upload de arquivos pelo método PUT, com as seguintes restrições:

1.3.5.39.1. Tamanho por arquivo.

1.3.5.39.2. Tamanho por conjunto de arquivos.

1.3.5.40. A criação das políticas deve possuir as formas:

1.3.5.40.1. Automático por meio da observação do tráfego para a aplicação.

1.3.5.40.2. Automático por meio da observação do tráfego de teste e manual.

1.3.5.41. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

1.3.5.41.1. Assinatura de ataque.

1.3.5.41.2. Código de response.

1.3.5.41.3. Conteúdo da cookie.

1.3.5.41.4. Conteúdo do cabeçalho.

1.3.5.41.5. Conteúdo do payload.

1.3.5.41.6. Horário.

1.3.5.41.7. Hostname.

1.3.5.41.8. IP de origem.

1.3.5.41.9. Método HTTP.

1.3.5.41.10. Número de ocorrências em determinado intervalo de tempo.

1.3.5.41.11. Parâmetro.

1.3.5.41.12. Tamanho da resposta de uma página web.

1.3.5.41.13. Tipo de protocolo (HTTP ou HTTPS).

1.3.5.41.14. User-agent (navegador).

1.3.5.41.15. Usuário.

1.3.5.42. Permitir a criação de assinaturas de ataques.

1.3.5.43. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

1.3.5.43.1. Ataques de negação de serviços automatizados.

1.3.5.43.2. Worms e vulnerabilidades conhecidas.

1.3.5.43.3. Requests em objetos restritos.

1.3.5.44. Prevenir contra vazamentos dos códigos dos servidores.

1.3.5.45. Proteger contra as 10 maiores vulnerabilidades da lista OWASP.

1.3.5.46. Exportar requisições que contém os ataques, nos formatos PDF e CSV.

1.3.5.47. Realizar localização geográfica do IP, identificando pais de origem da requisição.

1.3.5.48. Aprender o comportamento da aplicação:

1.3.5.48.1. Campos, valores, cookies e URLs.

1.3.5.48.2. Políticas sugeridas somente devem ser aplicadas após um período configurável.

1.3.5.49. Inspecionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses.

1.3.5.50. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP.

1.3.5.51. Proteger contra mensagens XML e SOAP malformadas.

1.3.5.52. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT.

1.3.5.53. Suportar SSL offload.

1.3.5.54. Remove as mensagens de erro do conteúdo que será enviado aos usuários.

1.3.5.55. Emitir os seguintes relatórios:

1.3.5.55.1. Gráfico indicando tipo de ataque.

1.3.5.55.2. Gráfico indicando tipo de violação.

1.3.5.55.3. Gráfico indicando quais URLs foram atacadas.

1.3.5.55.4. Gráfico indicando severidade.

1.3.5.55.5. Gráfico indicando os endereços IPs de origem.

1.3.5.55.6. Gráfico indicando a localização geográfica dos endereços IPs de origem.

1.3.5.56. Permitir a seleção de período para emissão dos relatórios, sendo que devem estar disponíveis os dados dos últimos 90 (noventa) dias.

1.3.5.57. Possuir console de administração com interface gráfica remota segura, a partir de plataforma Windows 7 e Windows XP, atendendo os seguintes requisitos:

1.3.5.57.1. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs.

1.3.5.57.2. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster.

1.3.5.57.3. Permitir a geração das seguintes informações, por período:

1.3.5.57.3.1. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário.

1.3.5.57.3.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas.

1.3.5.57.3.3. Informações estatísticas de fluxo de tráfego.

1.3.5.57.3.4. informações estatísticas de quantidade de sessões ou conexões.

1.3.5.58. Caso a solução de firewall de aplicação exija servidor físico de uso genérico para a execução de qualquer de suas funcionalidades, o equipamento ofertado deverá atender aos seguintes requisitos:

- Servidor tipo rack, para instalação em rack padrão de 19", limitado a 2U de altura.
- Possuir pelo menos 1 (um) processador de 8 (oito) núcleos, arquitetura de 64 bits.
- Possuir pelo menos 32GB de memória RAM DDR3.
- Possuir pelo menos 2 (dois) discos internos com configuração mínima de 300 GB, tecnologia SAS, velocidade de 10.000 RPM.
- Possuir pelo menos 2 (duas) portas GbE 1000Base-T.
- Possui fonte de alimentação 220V, redundantes N+1.

ANEXO II – RESUMO DO AMBIENTE TECNOLÓGICO DO CJF

1. Princípios

1.1. A plataforma de hardware e software do ambiente implantado no CJF e a metodologia para administração adotada visam atender, prioritariamente, os seguintes princípios:

1.1.1. **Escalabilidade,** possibilitando o crescimento modular.

1.1.2. **Capacidade,** viabilizando o gerenciamento de grandes volumes de dados e tabelas.

1.1.3. **Conectividade,** permitindo o acesso aos dados por usuários internos e externos ao CJF, a partir de protocolos de rede múltiplos.

1.1.4. **Desempenho,** garantindo o acesso simultâneo de número expressivo de usuários do CJF e de instalações externas, governamentais ou não.

1.1.5. **Disponibilidade,** dotando o ambiente corporativo de um nível aceitável de tolerância a falhas.

1.1.6. **Continuidade,** normatizando e divulgando às áreas responsáveis os procedimentos e processos de execução dos serviços, mediante documentação organizada e padronizada.

1.1.7. **Controle,** efetuando registros de todos os problemas, alterações e implementações realizadas no ambiente computacional.

1.1.8. **Segurança,** prevendo mecanismos de controle de acesso às informações e ferramentas que garantam a integridade e confiabilidade dos dados.

1.1.9. **Governança,** adequando todos os procedimentos, processos, documentações e execução de serviços em plena compatibilidade com as melhores práticas utilizadas pelo mercado ou com modelos adotados pelo CJF.

1.2. A empresa contratada deverá prestar os serviços considerando o ambiente atual do CJF, composto das tecnologias especificadas nos itens 2 e 3 abaixo (hardware e software respectivamente).

2. Plataforma de Hardware

A CONTRATADA deverá fornecer a solução (juntamente com a documentação) que seja compatível e adequada obrigatoriamente à infraestrutura tecnológica do Conselho de Justiça Federal descrita no quadro abaixo:

Tipo do Ativo	Marca / Modelo do Ativo	Descrição	Quantidade
Servidores Rack	IBM / RS6000	Servidor 4GB HD, 1 GB de memória, 1 Processador RISC Power4, 1 Unidade Fita DAT	1
	IBM RISC pSeries p630 - 7028-6C4	Servidor 4x 36GB HD, 12 GB de memória, 4 Processadores RISC Power4+, 1 Unidade fita DAT.	2
	IBM / xSeries 236	Servidor 6x86GB HD, 3 GB de memória, 2 Processadores Xeon, 1 Unidade Fita DAT.	1
Videoconferência	Radvsion / Scopia 24	Unidade de Controle Multiponto (MCU).	2
	HP / DL160	Servidor 4GB HD, 4 GB de memória, 2 Processadores Xeon Quad Core.	4
	Sony / PCS-G50	Equipamento de videoconferência (Codec) .	25
Servidores Blade	Dell / PowerEdge M600	Servidor de dois processadores de núcleo quádruplo com 32GB de RAM.	22
	Dell / PowerEdge M610	Servidor de dois processadores de núcleo quádruplo com 32GB de RAM.	5
Storages	NetApp / FAS3140	2 Controladoras e uma capacidade de 70T bruto sendo 9 shelves com discos FC e SATA. Suporte para FCP, NFS, HTTP. Data-on-Tap 7.3.3.	1
	NetApp / FAS2040	2 Controladoras e uma capacidade de 40T bruto sendo 3 shelves com discos FC e SATA. Suporte para FCP, NFS, HTTP. Data-on-Tap 7.3.3	1
Tape Library (Bibliotecas Robotizadas)	IBM / TS3310	Biblioteca composta por 2 drives, com capacidade para 30 fitas LTO3, conexão via Fibre Channel.	1
	QUANTUM / Scalar i500	Biblioteca composta por 4 drives LTO 5, com capacidade para 179 fitas LTO5, conexão via Fibre Channel.	
Racks de Servidores	Dell 42U	Racks p/Servidores/Libraries/Unid. Fita	2

Tipo do Ativo	Marca / Modelo do Ativo	Descrição	Quantidade
	NetApp 42U	Racks p/Servidores/Libraries/Unid. Fita	1
	Black Box 40U	Racks p/Servidores/Libraries/Unid. Fita	3
Racks de Comunicação	Embratel 40U	Rack 40U p/Ativos de Rede	1
	Furukawa 40U	Rack 40U p/Ativos de Rede	1
Switches de Convergência	EMC / MP8000B	2 switchs FCoE topo de rack com 32 portas sendo 8 FC de 8Gb/s e 24 Ethernet de 10Gb/s para rede local Storage/Blade	2
Switches de Core	H3C / S7506E	Concentradores da Rede Local 48 Portas Ethernet 10/100/1000 Mbps, 2 módulos de comunicação 10GB com 8 portas cada, 2 módulos Compat Flash com 2 portas 10GB	2
Switches de Acesso	H3C / S5500	Switchs ethernet 24 portas 10/100/1000 Mbps com Uplink 10Gbps e alimentação redundante	29
Controlador Rede Wireless	H3C / WX2200	Switch para Gerência Wireless com 3 portas	1
Access Points (APs)	H3C / AP3950	Acesso Rede Wireless 802.11a/b/g/n	25
Equipamentos da Solução Segurança	Fortigate 1000A	Segurança UTM composta de 2 Fortigate com 10 portas 1000Mbps e 1 FortiAnalizer para gravação de logs	3

3. Plataforma de Software

Para efeito de dimensionamento das licenças necessárias para a solução de gestão de vulnerabilidades (Item 1.2), deve ser considerado as seguintes versões e quantitativo de softwares :

Software	Nome / Versão	Quantidade
Servidores Aplicações	Tomcat	22
	Apache	39
	PHP	37
	IIS	4
	Jboss	1
	Oracle AS	5
	Zope/plone	9

Conselho da Justiça Federal

Gerenciador de Banco de Dados e ferramenta ETL	BD Oracle	3
	Ingres	2
	MySQL	3
	BRS	3
	MS SQL Server	1
	Postgres	6
Sistema Operacional	Windows XP	1
	Windows 7	1
	Windows Server 2003	1
	Windows Server 2008 32 bits	4
	Windows Server 2003 Enterprise	13
	Windows Server 2008 64 bits	3
	Windows Server 2008 R2 Enterprise	6
	Windows XP Professional	1
	Suse Linux Enterprise Server 10	43
	Suse Linux Enterprise Server 11	87
	Suse Linux Enterprise Server 9	7

O quadro a seguir apresenta os sistemas operacionais, aplicativos, softwares de gerência, SGBDs, servidores de aplicação, servidores web e ferramentas em uso no CJF:

Software	Nome / Versão	Descrição
Sistema Operacional	MS / Windows 2003 e 2008 Server.	Sistema Operacional de 32 bits e 64 bits

Software	Nome / Versão	Descrição
	MS / Windows XP Prof. (Port)	Sistema Operacional de 32 bits
	Suse / Linux 9, 10 e 11	Sistema Operacional de 32 bits
	IBM AIX 6.1	Sistema Operacional de 32 bits
Servidores Aplicações	IIS 6.0(Internet Information Services)	Servidor de Aplicações Microsoft ASP / HTML
	Apache 2.2.15	Servidor de Aplicações Apache / PHP
	Tomcat 5	Servidor de Aplicações Java
	OAS 10g	Servidor de Aplicações Oracle
	Plone / Zope	Servidor de Aplicações Zope
	Jboss 4.2.3	Servidor de Aplicações Jboss Java
Aplicativos	MS / Office 2007	Suite de Aplicativos para Escritório
	Internet Explorer # 7	Software de Navegação Internet (Browser)
Softwares / Ferramentas de Gerência / Administração / Monitoração	PHPLDAPADMIN 1.2.0.5	Ferramenta de Administração de Open LDAP
	WEBMIN 1.350	Ferramenta de Administração de Servidores
	AWSTATS 6.7	Ferramenta de Estatística de Sites
	ZABBIX 1.8.5	Software de Monitoramento do Ambiente
	TSM - Tivoli Storage Manager 5.5	Software de Gerenciamento de Backup
	SPAMASSASSIM / MailScanner 4.78.17	Ferramenta de Antispam
	Fortigate 1000A	Solução de Segurança para Rede Corporativa (Firewall, IPS, Filtro de Conteúdo Web, VPN)
	XenCenter 6.0.2	Ferramenta de Virtualização de Servidores
	OfficeScan 10.5	Solução de antivírus
	Jabber – OpenFire 3.6.4	Administração Chat
	Cacti 0.8.7b	Ferramenta de Estatística de Utilização de Rede

Software	Nome / Versão	Descrição
	Windows Media Services 9.0	Serviço de Streaming de Video
	Metaframe Presentation Server 4.0	Ferramenta para Acesso Remoto
Gerenciador de Banco de Dados e ferramenta ETL	Postgres 8.1.9	Sistema gerenciador de banco de dados Postgres
	MySql 5.0.26	Sistema gerenciador de banco de dados MySql
	SqlServer 2008	Sistema gerenciador de banco de dados SqlServer
	Ingres II 10.0.0	Sistema gerenciador de banco de dados Ingres
	Brs 8.0	Sistema gerenciador de banco de dados Brs
	Oracle 11g	Sistema gerenciador de banco de dados Oracle
	ODI 10 / Sunopsis	Ferramentas ETL Oracle Data Integrator e Sunopsis
Solução de Gerenciamento de Identidades e Controle de Acesso	Novell Identity Manager 2.7 Novell Access Manager 2.6.0 Novell iManager 2.7.0 Provisioning Module for Novell Identity Manager 2.7 Microsoft Active Directory 2008	Solução de Gerenciamento de Identidades e Controle de Acesso
Servidores Web	IIS 6.0(Internet Information Services).	Servidor de Web
	Apache 2.2.15	Servidor de Web
	Tomcat 5	Servidor de Web
	Jboss 4.2.3	Servidor de Aplicações Jboss.org
	OAS 10g	Servidor de Web
	IMAP 4.1.3	Servidor de POP IMAP Courier
	PostFix 2.4.3	Servidor de SMTP
	Squid 3.1.1	Servidor de Webcache

Software	Nome / Versão	Descrição
	Open LDAP	Servidor de Diretórios
	Dansguardian 2.9.8.0	Servidor de Bloqueio de Conteúdo

ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO DA SOLUÇÃO

ETAPA ÚNICA: ENTREGA, INSTALAÇÃO E CONFIGURAÇÃO DOS EQUIPAMENTOS E SOFTWARES DA SOLUÇÃO		
Prazo Máximo (em dias corridos)	*Descrição*	**Responsável**
D	Data de emissão de Ordem de Serviço – OS dos equipamentos, softwares e serviços da solução pelo CONTRATANTE.	CJF
D + 3	Reunião de Planejamento.	CJF e CONTRATADA
D + 30	Entregar o Plano de Implantação contendo o planejamento das atividades para as etapas de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução.	CONTRATADA
D + 30	Comprovar que os técnicos que executarão as atividades são certificados pelos fabricantes dos componentes da solução.	CONTRATADA
	Aprovar o Plano de Implantação para as etapas de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução.	CJF
D + 45	Concluir a entrega dos equipamentos, softwares e acessórios, juntamente com toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização e os demais documentos.	CONTRATADA
	Emitir o **Termo de Recebimento Provisório (TRP)** após a entrega dos equipamentos, softwares, Plano de Implantação aprovado e demais documentações da solução. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.	CJF
Data de Emissão do TRP + 60	Concluir, a partir da data de emissão do Termo de Recebimento Provisório (TRP), os serviços de instalação e configuração dos equipamentos e softwares da solução integrada de segurança, realizando todas as atividades programadas para esta etapa.	CONTRATADA
	Emitir o **Termo de Recebimento Definitivo (TRD)** após a finalização dos serviços de instalação e configuração, acompanhado da documentação técnica detalhada de todos os procedimentos executados, desde que não haja pendências a cargo da CONTRATADA.	CJF

Data de Emissão do TRD + 30	Realizar o acompanhamento ON-SITE da operação inicial da solução integrada de segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução.	CONTRATADA

ANEXO IV – TERMO DE CONFIDENCIALIDADE E SIGILO DA LICITANTE

1. A empresa [RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Conselho da Justiça Federal – CJF, aceita as regras, condições e obrigações constantes do presente Termo.

2. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CJF reveladas à EMPRESA RECEPTORA em função da vistoria prévia realizada para atendimento ao Edital do Pregão Eletrônico n.º XX/2013.

3. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

4. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CJF, das informações restritas reveladas.

5. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CJF, as informações restritas reveladas.

6. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CJF, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

7. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CJF qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CJF, possibilitará a imediata rescisão de qualquer contrato firmado entre o CJF e a EMPRESA RECEPTORA sem qualquer ônus para o CJF. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, ao

pagamento ou recomposição de todas as perdas e danos sofridos pelo CJF, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CJF.

E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Brasília, de de 2013.

_____
ASSINATURA DO RESPONSÁVEL TÉCNICO / REPRESENTANTE

_____
CARIMBO E ASSINATURA DO REPRESENTANTE DO CJF

ANEXO V – TERMO DE CONFIDENCIALIDADE E SIGILO DA CONTRATADA

1. A empresa [RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Conselho da Justiça Federal – CJF, aceita as regras, condições e obrigações constantes do presente Termo.

2. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CJF reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do contrato n.º XX/2013.

3. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

4. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CJF, das informações restritas reveladas.

5. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CJF, as informações restritas reveladas.

6. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CJF, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

7. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.
8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CJF qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CJF, possibilitará a imediata rescisão de qualquer contrato firmado entre o CJF e a EMPRESA RECEPTORA sem qualquer ônus para o CJF. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, além das multas definidas no Termo de Referência, ao pagamento ou recomposição de

todas as perdas e danos sofridos pelo CJF, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CJF.

11. E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Brasília, de de 2013.

_____
ASSINATURA DO REPRESENTANTE DA CONTRATADA

_____
CARIMBO E ASSINATURA DO REPRESENTANTE DO CJF

Conselho da Justiça Federal

MÓDULO II DO PREGÃO ELETRÔNICO n. 26/2013

ESPECIFICAÇÃO DO OBJETO/PLANILHA DE PREÇOS

CNPJ:
Razão Social:
Endereço:
Telefone(s): ( ) Fax: ( ) E-mail:
Banco: Agência: C/C:
Validade da Proposta: ___/___/_____ Prazo de Entrega:

Item	Subitem	DESCRIÇÃO	Qtd.	Descrever os nomes dos produtos que compõe a solução	Preço Unitário (R$)	Preço Total (R$)
Único	1.1	Solução de Gerenciamento de Ameaças, com garantia por 48 meses	01			
	1.2	Solução de Gestão de Vulnerabilidades, com garantia por 48 meses	01			
	1.3	Solução de Firewall de Aplicação, com garantia por 48 meses	01			
	VALOR TOTAL EQUIPAMENTOS					
	1.4	Serviço de Instalação e configuração da Solução (parcela única)	01			
	1.5	Serviço de Suporte Técnico pelo período de 48 meses (valor mensal e total)	48			
	1.6	Transferência de Conhecimento (por pessoa)	04			
	VALOR TOTAL DOS SERVIÇOS					
	VALOR TOTAL GERAL DA SOLUÇÃO					

Observações

1. É obrigatório as empresas licitantes preencherem integralmente esta planilha de preço.
2. Os custos relativos ao serviço de garantia dos equipamentos e softwares que compõe a solução **já devem estar incluídos no preço dos próprios itens.**
3. A CONTRATADA deverá emitir Nota Fiscal/Fatura relativa aos valores dos equipamentos e softwares da solução e garantia por 48 (quarenta e oito) meses, serviços de instalação e configuração e serviço de transferência de conhecimento após receber cópia do Termo de Recebimento Definitivo previsto no Cronograma (ANEXO III).
4. O pagamento do serviço de Suporte Técnico será efetuado mensalmente, sendo iniciado somente após o Recebimento Definitivo da Solução, mediante envio da Nota Fiscal/Fatura pela CONTRATADA.

MÓDULO III DO PREGÃO ELETRÔNICO n. 26/2013
MINUTA DE CONTRATO

CONTRATO CJF N.º ____/2013

CONTRATO DE FORNECIMENTO E PRESTAÇÃO DE SERVIÇO QUE ENTRE SI CELEBRAM O CONSELHO DA JUSTIÇA FEDERAL E A EMPRESA _____, NA FORMA E CONDIÇÕES A SEGUIR:

A **UNIÃO,** por intermédio do **CONSELHO DA JUSTIÇA FEDERAL**, Órgão integrante do Poder Judiciário da União, inscrito no CNPJ sob o nº 00.508.903/0001-88, com sede no SCES LOTE 09, TRECHO III, POLO 08, PRÉDIO DO CONSELHO DA JUSTIÇA FEDERAL, Brasília-DF, doravante denominado **CONTRATANTE**, neste ato representado por sua Secretária-Geral, Dra. EVA MARIA FERREIRA BARROS, brasileira, solteira, inscrita no CPF sob o nº _____, portadora da Cédula de Identidade nº _____, expedida pela _____ residente e domiciliada nesta Capital, e a empresa _____, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº _____, com sede no _____, aqui denominada **CONTRATADA**, neste ato representada por seu Diretor _____, Senhor _____, brasileiro, _____, _____, inscrito no CNPJ sob o nº _____, portador da Cédula de Identidade nº _____, expedida pela _____, residente e domiciliado _____, CELEBRAM, com fundamento na Lei nº 10.520, de 17 de julho de 2002, no Decreto nº 5.450/2005, Resolução n. 98 de 10 de novembro de 2009 do Conselho Nacional de Justiça,Lei Complementar 123/2006 e subsidiariamente na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Processo **ADM-2012/00420**, o presente **CONTRATO DE FORNECIMENTO E PRESTAÇÃO DE SERVIÇOS** mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por objeto a Contratação de solução integrada de segurança, contemplando o fornecimento de equipamentos, softwares e sistemas de gerenciamento da solução, com garantia de 48 meses e serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades do Conselho da Justiça Federal - CJF, de acordo com as especificações técnicas contidas nos Módulos I - Termo de Referência e seus Anexos e II - Planilha.

1.2. <u>O detalhamento do objeto é apresentado no Módulo I –Termo de Referência e seus anexos, o qual adere a este contrato e dele faz parte, independentemente de transcrição</u>

CLÁUSULA SEGUNDA – DA ENTREGA, INSTALAÇÃO E CONFIGURAÇÃO DOS EQUIPAMENTOS E SOFTWARES DA SOLUÇÃO.

2.1. A CONTRATADA deverá:

2.1.1 Entregar dos equipamentos, softwares e acessórios da solução e a realização dos serviços previstos neste Contrato deverão ser realizados na sede do Contratante, situada no Setor de Clubes Esportivos Sul – SCES - Trecho III, Pólo 08, Lote 09 – CEP 70200-003 - Brasília-DF.

2.1.2. Os modelos e versões dos equipamentos (hardware) que compõe a solução integrada de segurança deverão ser ofertados novos, sem uso anterior, e deverão permanecer em linha de

produção pelos próximos 12 (doze) meses, contados da entrega dos equipamentos, e com previsão de suporte pelos próximos 5 (cinco) anos, contados da data de assinatura do Contrato.

2.1.3. Todos os equipamentos e softwares especificados deverão ser adquiridos em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo com o término do contrato.

2.1.4. Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança de acordo com os prazos definidos no cronograma constante do Anexo III do Módulo I, parte integrante deste contrato.

2.1.4.1 No 3º (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na SEDE do CONTRATANTE, com o objetivo de apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução integrada de segurança.

2.1.4.2 A CONTRATADA deverá apresentar um Plano de Implantação, em até 30 (trinta) dias da emissão da Ordem de Serviço pelo CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução integrada de segurança.

2.1.5. Entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até 45 (quarenta e cinco) dias, a contar da data de emissão da Ordem de Serviço pelo CONTRATANTE.

2.1.6 Entregar os equipamentos novos e de 1º uso, no prazo indicado na alínea anterior, juntamente com todos os itens acessórios de hardware e de software necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração, conforme especificações constantes do ANEXO I deste Termo de Referência.

2.2. O plano de Implantação conterá no mínimo, os requisitos constantes do **Subitem 5.2.4** do Anexo III do Módulo I, parte integrante deste contrato.

2.3. As demais obrigações da CONTRATADA em relação a entrega, instalação e configuração da solução estão descritas nos subitens 5.2.7 ao 5.2.21.1 do Termo de Referência, Módulo I do edital, parte integrante deste Contrato.

CLÁUSULA TERCEIRA – DA TRANSFERÊNCIA DE CONHECIMENTO

3.1 A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do Contratante por meio de treinamento nas tecnologias da solução com carga horária total mínima de 80 (oitenta) horas.

3.2 A transferência de conhecimento deverá ser realizado em Brasília-DF cabendo a CONTRATADA providenciar as instalações para este fim.

3.3 As demais obrigações da CONTRATADA em relação as especificações da transferência de conhecimento estão descritas nos subitens 5.3.3 ao 5.3.10 do Termo de Referência, Módulo I do edital, parte integrante deste Contrato.

CLÁUSULA QUARTA – DA GARANTIA E SUPORTE TÉCNICO

Garantia da Solução

4.1. O prazo de garantia dos equipamentos e direito a atualização dos softwares que compõe a solução é de 48 (quarenta e oito) meses, contados a partir da data de aceitação pelo

CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução.

4.1.1. Os custos relativos ao serviço de garantia dos equipamentos e softwares que compõe a solução já devem estar inclusos no preço dos próprios itens.

4.2. O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento dos equipamentos, dos softwares e na integração entre os componentes da solução, mediante a substituição de equipamentos e versões dos softwares ou revisão de configurações, de acordo com as recomendações dos fabricantes, informações presentes nas páginas e manuais de suporte e normas técnicas específicas:

4.3. O direito a atualização dos softwares obriga a CONTRATADA a disponibilizar a atualização de bases externas de categorização de sites, mensagens, vírus, malware, assinatura de ataques e vulnerabilidades, bem como dos demais softwares fornecidos e que compõe a solução, tão logo ocorra o lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.

4.4. A reparação de falhas de funcionamento dos componentes da solução deverá ocorrer de acordo com o **Subitem 5.4.5 do Termo de Referência, Módulo I** do edital, parte integrante deste Contrato.

4.5. A atualização dos softwares fornecidos que compõe a solução deverá ocorrer de acordo com o **Subitem 5.4.6 do Termo de Referência, Módulo I** do edital, parte integrante deste Contrato.

4.6 Juntamente com a documentação de entrega, instalação e configuração da solução, como requisito para a emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

4.6.1 Certificado de garantia de que todos os equipamentos que compõe a solução estão cobertos por garantia e suporte técnico on-site, diretamente do fabricante, com prazo de solução de até 8 (oito) horas, pelo período de 48 (quarenta e oito) meses totais exigidos no item 4.1.

4.6.1.1 Caso não seja comercializado item de garantia com o prazo nos moldes exigidos no item anterior, deverá ser entregue pela CONTRATADA declaração oficial, emitida pelo fabricante dos equipamentos, atestando a contratação do serviço de garantia e suporte técnico on-site com o nível de serviço e duração solicitados.

4.6.2. Cessões de direito de uso perpétuo dos softwares fornecidos. Os termos de licenciamento de todos os softwares fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão direito pertencentes ao CONTRATANTE.

4.6.3 Conjunto de direitos de atualização de versão, pelo período de 48 meses de garantia, de todos os softwares fornecidos. Abrangerá todos os softwares e licenças a serem fornecidos na solução. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e comporão direito pertencente ao patrimônio do CONTRATANTE.

Suporte Técnico da Solução

4.7. O serviço de suporte técnico on-site para os equipamentos e softwares que compõe a solução deverá ser executado pela CONTRATADA ou diretamente pelo fabricante, durante o prazo de 48 (quarenta e oito) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução.

4.8 O serviço de suporte técnico da solução consiste em:

4.8.1. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visando à solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução (equipamentos e softwares), permitindo o retorno à condição normal de operação.

4.8.2. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou outro recursos de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução.

4.8.3. Realizar visitas técnicas preventivas no local de instalação da solução (on-site), com frequência mensal, e com duração de pelo menos 8 (oito) horas a cada visita, visando assegurar o melhor desempenho da solução.

4.8.4. Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas.

4.9. Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, os chamados deverão ser categorizados em 4 (quatro) níveis, da seguinte forma:

Criticidade	Descrição	Prazo máximo para início de atendimento (contados a partir da abertura do chamado)	Prazo máximo para restauração de serviço (contados a partir da abertura do chamado)
Severidade 1 (Alta)	Atuação ON-SITE visando sanar problemas que tornem a solução integrada de segurança inoperante, causando alto impacto nas operações de TI do CJF.	Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 6 (seis) horas
Severidade 2 (Média/Alta)	Atuação ON-SITE visando sanar problemas que prejudicam a operação normal da solução, mas não interrompem o acesso aos sistemas de TI, causando impacto no ambiente de produção ou restrição de funcionalidade.	Em até 4 (quatro) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 12 (doze) horas
Severidade 3 (Média/ Baixa)	Atuação REMOTA visando sanar problemas ou dúvidas que criem restrições a operação normal da solução integrada de segurança não gerando impacto ao negócio.	Em até 4 (quatro) horas um técnico da CONTRATADA entra em contato.	Em até 24 (vinte e quatro) horas
Severidade 4 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução integrada de segurança, ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 72 (setenta e duas) horas

4.10. As demais obrigações da CONTRATADA em relação as especificações do serviço de Suporte Técnico estão descritas nos subitens 5.5.4 ao 5.5.13 do Termo de Referência, Módulo I do edital, parte integrante deste Contrato.

CLÁUSULA QUINTA - DA RELAÇÃO EMPREGATÍCIA E DOS ENCARGOS SOCIAIS

5.1 - As partes desde já ajustam que não existirá para o CONTRATANTE qualquer solidariedade em relação ao cumprimento das obrigações trabalhistas e previdenciárias para com os empregados da CONTRATADA, destacados para executar os serviços, cabendo a esta assumir, de forma exclusiva, todos os ônus advindos da relação empregatícia, entre os quais os encargos provenientes de qualquer acidente que venha a vitimar um ou mais dos profissionais destacados, assim como por tudo mais quanto às leis sociais e trabalhistas lhes assegurem, inclusive férias, 13º salário, aviso-prévio, indenizações, etc.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES E RESPONSABILIDADES DAS PARTES

6.1 - Além das obrigações expressamente previstas neste Contrato e de outras decorrentes da natureza do ajuste, deverá a CONTRATADA**:**

a) fornecer os equipamentos e softwares da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CJF, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração;

b) acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Contrato.

c) submeter à prévia aprovação da CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços

d) manter, durante a execução deste contrato, as condições de habilitação e qualificação exigidos na licitação, particularmente no que tange à regularidade fiscal e à capacidade técnica e operativa;

e) sujeitar-se à fiscalização do CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer.

f) responsabilizar-se, pelos danos causados diretamente à Administração ou a terceiros, decorrente de sua culpa ou dolo na execução do presente contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Contratante, procedendo imediatamente aos reparos ou indenizações cabíveis e assumindo o ônus decorrente.

g) prestar as atividades objeto deste Contrato, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos equipamentos e softwares que compõem a solução integrada de segurança

h) não utilizar pessoal técnico já alocado em contratos ou projetos em execução no CONTRATANTE para prestar as atividades objeto deste Contrato, devendo compor equipe exclusiva para este fim

i) credenciar devidamente um Representante Técnico para, em todas as questões relativas ao cumprimento do objeto deste Contrato,representá-la.

j) indicar o profissional que atuará do início da execução deste Contrato até a conclusão da implantação como Gerente de Projeto, devendo possuir certificação PMP (Project Management Professional).

k) propor os ajustes necessários à adequação, segurança e racionalização dos serviços prestados, respeitando o objeto deste Contrato.

l) Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Contrato e seus Módulos, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias e demais exigências legais para o exercício da atividade objeto deste Contrato;

m) responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o

Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação das penalidades previstas, caso os prazos e condições não sejam cumpridas;

n) ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de pagamentos adicionais ao CONTRATANTE ou a não prestação satisfatória dos serviços

o) guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE

p) substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado

q) acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1º, da Lei nº 8.666/93, as solicitações do CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto licitado**;**

r) assumir a responsabilidade por danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do objeto licitado, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE.

s) sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe de Fiscalização e Recebimento indicada pelo CONTRATANTE para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas.

t) comunicar a Equipe de Fiscalização e Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços;

u) corrigir as falhas detectadas pela Equipe de Fiscalização e Recebimento indicada pelo CONTRATANTE

v) executar as atividades previstas no contrato em estrito cumprimento aos prazos previstos no ANEXO III – Cronograma de Implantação do Módulo I

x) manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações relativas à:

x.1) Política de segurança adotada pelo CJF e configurações de hardware e software decorrentes.

x.2) Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos em atendimento aos itens de segurança constantes do(s) objeto(s) instalado(s).

y) assinar Termo de Confidencialidade e Sigilo da Contratada (Anexo V do Módulo I), entregando o Termo assinado pelo representante legal da Contratada, com firma reconhecida.

6.2 - Poderá o CONTRATANTE, a qualquer tempo, exigir da CONTRATADA a comprovação das condições referidas na alínea "d" do item 6.1.

6.3 - Além das obrigações previstas neste Contrato e de outras decorrentes da natureza do ajuste, **deverá o CONTRATANTE**:

6.3.1. Acompanhar e fiscalizar a execução do objeto contratual;

6.3.2 Permitir o acesso dos técnicos habilitados e identificados da CONTRATADA, para os serviços inclusos no período de garantia, às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àquelas referentes à identificação, trânsito e permanência em suas dependências.

6.3.3. Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual;

6.3.4. Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados;

6.3.5. Comunicar formalmente qualquer anormalidade ocorrida na execução dos serviços pela CONTRATADA;

6.3.6. Avaliar todos os serviços prestados pela CONTRATADA;

6.3.7. Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal;

6.3.8. Indicar os seus representantes para fins de contato e demais providências inerentes à execução deste contrato;

CLÁUSULA SÉTIMA - DOS PREÇOS

7.1 - As partes ajustam que os preços a serem cobrados pelo fornecimento e instalação da solução bem como pela prestação de garantia, suporte técnico e pela transferência de conhecimento serão os constantes da Planilha de Preços – Módulo II do presente Contrato e da proposta apresentada pela CONTRATADA.

7.2 - Os preços firmados neste contrato para os subitens 1.1, 1.2, 1.3, 1.4, e 1.6, constante da Planilha de Preços são fixos e irreajustáveis.

7.3. O reajuste do suporte técnico, subitem 1.5 da planilha de preços, será efetuado conforme Cláusula 10 deste contrato.

CLÁUSULA OITAVA – DO RECEBIMENTO, DO PAGAMENTO E DAS GLOSAS

8.1. O recebimento e a aceitação do objeto deste Contrato obedecerão no que couber, ao disposto no Art. 73, inciso II, e seus parágrafos, art. 75 e 76 da Lei n.º 8.666/93.

8.2 – A solução será recebida por uma Comissão de Recebimento e Fiscalização composta por 3 (três) servidores da Secretaria de Tecnologia da Informação, auxiliada por 1 (um) servidor da Subsecretaria de Material e Patrimônio, na forma a seguir:

a) Provisoriamente: após entrega dos equipamentos, softwares, acessórios, Plano de Implantação aprovado e demais documentações da Solução, conforme descrito no cronograma do Anexo III do Módulo I, no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da Contratada, e desde que não haja pendências a cargo da mesma.

a.1) A entrega deverá ser formalizada mediante comunicação escrita da Contratada ao Contratante**.**

a.2) Concluir no prazo de 60 (sessenta) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação e configuração dos equipamentos e softwares da Solução Integrada de Segurança, realizando todas as atividades programadas para esta etapa.

b) Definitivamente: após a finalização instalação e configuração dos equipamentos e softwares da solução integrada de segurança, acompanhado da documentação técnica detalhada de todos os procedimentos executados, no prazo máximo de 15 (quinze) dias, desde que não haja pendências a cargo da Contratada, mediante a emissão do Termo de Recebimento Definitivo assinado pelas partes.

b.1) Realizar, por 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo (TRD), operação assistida ON-SITE da Solução Integrada de Segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução.

b.2) O serviço de operação assistida ON-SITE da Solução Integrada de Segurança deverá ser executado presencialmente nas instalações do Contratante, 8 (oito) horas por dia, durante o período normal de produção do ambiente de TI, compreendido das 07h às 20h.

8.3 - Constatadas irregularidades na solução quando da entrega, o Contratante poderá:

a) se disser respeito à especificação, rejeitá-lo no todo ou em parte, determinando sua substituição ou cancelamento do Contrato, sem prejuízo das penalidades cabíveis;

a.1) na hipótese de substituição a Contratada deverá providenciar sem que isso implique acréscimo aos preços contratados, a substituição em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas por outro novo e de primeiro uso, no prazo de 72 (setenta e duas) horas, independente do fato de ser ou não fabricante da solução fornecida.

a.2) a Contratada também deverá substituir, no prazo de 120 (cento e vinte) horas, qualquer equipamento, componente ou periférico por outro original e novo, caso seja constatada qualquer divergência com as especificações técnicas descritas na proposta técnica apresentada;

a.3) Em todas as hipóteses de substituição previstas anteriormente, caso exista a impossibilidade técnica de substituição por modelo igual, novo e original, será permitida a substituição por outro com características técnicas idênticas ou superiores, plenamente compatível, também original e novo.

b) se disser respeito à diferença de quantidade ou de partes, determinar sua complementação ou cancelamento do Contrato, sem prejuízo das penalidades cabíveis;

b.1) na hipótese de complementação, empresa deverá fazê-la em conformidade com a indicação da Secretaria de Tecnologia da Informação no prazo máximo de 5 dias úteis, contados da notificação por escrito, mantido o preço inicialmente contratado.

8.4 – O pagamento relativo aos valores dos equipamentos e softwares da solução, da garantia por 48 (quarenta e oito) meses, dos serviços de instalação e configuração e do serviço de transferência de conhecimento será efetuado somente após o recebimento do Termo de Recebimento Definitivo previsto no Cronograma (Anexo III do Módulo I deste Contrato), em parcela única.

8.4.1 - Este caracterizar-se-á pela emissão/juntada de Termo de Recebimento Definitivo emitido na forma do item 8.2 e aposição de Atesto no verso da Nota Fiscal de cobrança que ficará a cargo da Secretaria de Tecnologia da Informação do CONTRATANTE.

8.5. O pagamento do serviço de Suporte Técnico será efetuado mensalmente após envio da fatura pela CONTRATADA e aposição de Atesto no verso da Nota Fiscal de cobrança que ficará a cargo da Secretaria de Tecnologia da Informação do CONTRATANTE.

8.5.1. Os serviços de Suporte Técnico serão iniciados somente após o Recebimento Definitivo da Solução.

8.5.2 O pagamento será efetuado mediante apresentação de nota de cobrança consolidada para todos os equipamentos e softwares da solução, já descontadas as glosas eventualmente aplicadas em função do não atendimento dos níveis de qualidade definidos neste contrato, determinando o valor total do serviço para o mês.

8.5.3. Para os fins previstos no item **8.5** a CONTRATADA apresentará ao CONTRATANTE, até o quinto dia útil do mês subsequente a prestação do serviço, nota fiscal de cobrança.

8.6. A fim de que o CONTRATANTE possa efetuar o pagamento, a CONTRATADA deverá apresentar nota fiscal constando a indicação do banco, Agência e do número da Conta-corrente onde deverá ser efetuado o crédito.

8.7. As Notas Fiscais de cobrança deverão ser endereçadas à Seção de Segurança de Informações e Conformidade (SESIN) e entregues na Seção de Protocolo do CONTRATANTE, situada no SCES LOTE 09, TRECHO III, POLO 08, PRÉDIO DO CONSELHO DA JUSTIÇA FEDERAL, Brasília-DF**.**

8.7.1. Caso ocorra alteração no endereço informado no item 8.7, o CONTRATANTE oficiará à CONTRATADA do novo local de entrega das notas fiscais.

8.8. Apresentada a nota fiscal de cobrança na forma aqui estabelecida, terá o CONTRATANTE o prazo **máximo de 10 (dez) dias úteis** para efetuar o pagamento, contados a partir do recebimento definitivo.

8.9 Por ocasião dos pagamentos a CONTRATADA deverá comprovar a regularidade de sua situação para com o recolhimento das contribuições devidas ao INSS e ao FGTS, mediante apresentação das certidões respectivas além daquelas exigidas quando da contratação.

8.10. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação contratual sem que isso gere direito à alteração dos preços, ou de compensação financeira em face desta circunstância.

8.11. O depósito bancário produzirá os efeitos jurídicos da quitação da prestação devida.

8.12 Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, o valor faturado será atualizado monetariamente pelo percentual ***pro rata temporis*** do índice Geral de Preços Disponibilidade Interna – IGP/DI conhecido quando do faturamento, compreendido entre a data limite estipulado para pagamento e aquela em que se der o efetivo pagamento.

8.13 Também serão corrigidos na forma do item 8.12 os valores devidos pela CONTRATADA ao CONTRATANTE.

8.14. Caso a CONTRATADA deixe de apresentar a nota fiscal do serviço, os valores a serem posteriormente cobrados serão os vigentes na data da ocorrência do serviço.

8.14.1 O pagamento efetivado na forma aqui mencionado não gera direito ao pleito de reajustamento de preços ou correção monetária.

8.15 – Poderá o CONTRATANTE, após efetuar análise da(s) nota(s) fiscal(is) de cobrança, efetuar glosas sobre os valores cobrados, conforme descrito no item 11 do Módulo I – Termo de Referência, Anexo deste Contrato.

8.15.1. Independentemente das penalidades previstas na Cláusula Décima deste contrato, será aplicado redutor de fatura (GLOSA) pelo não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico, nos seguintes casos:

a) Glosa de 5% (cinco por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade alta**, limitada até 06 (seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

b) Glosa de 3% (três por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade média/alta**, limitada até 12 (doze) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

c) Glosa de 2% (dois por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade média/baixa**, limitada até 18 (dezoito) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

d) Glosa de 1% (dois por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade baixa**,

limitada até 36 (trinta e seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

8.15.2 – Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas previstas a cada ocorrência, a CONTRATADA receberá uma Sanção de Advertência, a ser aplicada pela área Administrativa do CONTRATANTE.

8.15.3 - A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços.

8.15.4 - Ocorrendo glosa, esta será deduzida da própria nota fiscal de cobrança, devendo o CONTRATANTE oficiar à CONTRATADA sobre as razões que ensejaram o desconto.

8.16 No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses, serão aplicadas as Sanções Administrativas previstas no Contrato.

8.17 No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa.

8.18 Se a decisão da Administração for favorável ao recurso da CONTRATADA, a mesma emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

8.19 A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

8.20. Deverão ser novamente cobrados, com os valores vigentes à época da primeira cobrança, as quantias que tenham sido descontadas indevidamente.

CLÁUSULA NONA – DA VIGÊNCIA

9.1 – A vigência deste Contrato será de 52 (cinquenta e dois) meses, sendo:

a) 04 (quatro) meses, contados da emissão da Ordem de Serviço, destinados a entrega, instalação, configuração e transferência de conhecimento;

b) 48 (quarenta e oito) meses, contados da data do Termo de Recebimento Definitivo, referente à garantia e suporte técnico da solução integrada de segurança.

CLÁUSULA DÉCIMA - DO REAJUSTE

10.1. O preço a que se refere o item 7.3 (Suporte Técnico) deste instrumento, poderá ser reajustado decorrido doze meses de vigência do Contrato, mediante negociação entre as partes, tendo como limite máximo a variação do IGP-DI ocorrida nos doze meses anteriores ao reajuste, contados da assinatura do contrato.

CLÁUSULA DÉCIMA PRIMEIRA - DO VALOR DO CONTRATO E DA DOTAÇÃO ORÇAMENTÁRIA

11.1. O valor do presente contrato é de R$ _____ (_____).

11.2. As despesas com a execução deste contrato serão atendidas, no exercício de 2013, com os recursos consignados no Orçamento Geral da União e suplementações a ele incorporadas, no Programa de Trabalho 000.821 e Elemento de Despesa 33.90.39.

11.3. Foi emitida a Nota de Empenho n.º 2013NE000___, no valor de R$ _____ (_____) à conta da dotação orçamentária especificada no item 11.2 deste contrato.

11.4. Observada as limitações constantes do § 1º do artigo 65 da Lei n.º 8.666/93 poderá o CONTRATANTE, promover alterações no objeto do presente contrato.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

12.1. Para os fins previstos no art. 86 e 87 da Lei 8.666/93, pela inexecução total ou parcial das obrigações assumidas a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as seguintes sanções.

12.1.1 Advertência;

12.1.2. Multa no percentual correspondente a 0,05% (cinco centésimos por cento), calculada sobre o valor total da contratação, **por dia de atraso na entrega do plano de implantação**, além do prazo máximo definido no CRONOGRAMA (Anexo III do Módulo I parte integrante deste contrato), até o limite de 30 (trinta) dias corridos.

12.1.3. Multa no percentual correspondente a 0,1% (um décimo por cento), calculada sobre o valor total da contratação, **por dia de atraso na entrega de todos os equipamentos, softwares e acessórios da solução**, além do prazo máximo definido no CRONOGRAMA (Anexo III do Módulo I parte integrante deste contrato), até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

12.1.4. Multa no percentual correspondente a 0,15% (quinze décimos por cento), calculada sobre o valor total da contratação, **por dia de atraso na conclusão da etapa de instalação e configuração da solução**, além dos prazos máximos definidos no CRONOGRAMA (Anexo III do Módulo I parte integrante deste contrato) até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

12.1.5. Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total do serviço de transferência de conhecimento, **por dia de atraso na conclusão do serviço de transferência de conhecimento**, além do prazo máximo definido no CRONOGRAMA (Anexo III do Módulo I parte integrante deste contrato), até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

12.1.6. Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total da contratação, **no caso de aplicação de glosa referente ao mesmo indicador de Nível Mínimo de Serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses**, caracterizando inexecução parcial do contrato.

12.1.7. Multa no percentual correspondente a 0,01% por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor total do contrato, **no caso de atraso injustificado no credenciamento do representante**, constante no item 5.1.8 do Módulo I – termo de Referência, parte integrante deste contrato.

12.1.8. Multa no percentual correspondente a 0,20% por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor da garantia contratual disposta na Cláusula Décima Terceira deste contrato, **no caso de atraso injustificado na sua entrega.**

12.1.9. A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da multa, no percentual de 20% (dez por cento) sobre o valor da parte não entregue ou não executada.

12.1.10. Multa no valor de 5% (cinco por cento), sobre o valor total da contratação, **no caso de inexecução total do contrato**.

12.1.11. O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos artigos 87 e 88 da Lei n. 8.666/1993.

Conselho da Justiça Federal

12.2. O valor da multa aplicada, após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pelo CONTRATANTE, descontado da garantia contratual ou cobrado judicialmente.

12.3. A reincidência da aplicação de multa ou advertência dará direito ao CJF à rescisão contratual unilateral.

12.4. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

12.5. A critério da autoridade competente do Conselho, com fundamento nos Princípios da Proporcionalidade e Razoabilidade, as penalidades poderão ser relevadas ou atenuadas, em razão de circunstâncias fundamentadas em fatos reais e comprovados e desde que formuladas, por escrito, no prazo máximo de 05 (cinco) dias úteis, contado da data em que for oficiada da pretensão no sentido da aplicação da pena.

12.6. Quem, convocado dentro do prazo de validade da sua proposta, não assinar a Ata e celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e, será descredenciado no Sicaf, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do Art. 4º da Lei 10.520/02, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e das demais cominações legais.

CLÁUSULA DÉCIMA TERCEIRA - DA GARANTIA

13.1 – Para o integral cumprimento de todas as obrigações ora assumidas, inclusive indenização a terceiros e multas eventualmente aplicas, a CONTRATADA entregará ao CONTRATANTE**,** no prazo máximo de 20 (vinte) dias contados da data da assinatura deste contrato, garantia no valor de R$....., correspondente a 5% (cinco por cento) do valor do contrato, nos termos do artigo 56, § 2º da Lei nº 8.666/93.

13.2 – O CONTRATANTE poderá descontar da garantia os valores que a CONTRATADA passe a lhe dever em virtude de ocorrência de qualquer das situações previstas neste contrato ou dele decorrentes.

13.3 – Caso o valor da garantia venha ser utilizado em pagamento de qualquer obrigação, desde que atribuída à CONTRATADA**,** esta se obriga a efetuar a respectiva reposição no prazo máximo de 48 (quarenta e oito) horas, contado do recebimento da comunicação do CONTRATANTE**.**

13.4. A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expirar o vencimento, alteração por aumento no valor do contrato ou outra necessidade indispensável.

13.6. Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ao até mesmo restrinjam-lhe a cobertura ou a sua eficácia.

13.7. O termo da garantia será restituído à CONTRATADA depois de encerrada a vigência contratual e após o cumprimento integral de todas as obrigações contratuais.

CLÁUSULA DÉCIMA QUARTA - DA RESCISÃO

14.1. O presente contrato poderá ser rescindido ocorrendo uma ou mais hipóteses previstas no art. 77 e seguintes da Lei nº 8.666/93, o que a CONTRATADA declara expressamente conhecer.

14.2. Na hipótese da rescisão ser procedida por culpa da CONTRATADA, fica o CONTRATANTE autorizado a reter, até o limite dos prejuízos experimentados, os créditos a que aquela tenha direito.

14.2.1. Inexistindo créditos em favor da CONTRATADA ou sendo estes insuficientes para fazer face ao montante dos prejuízos, o CONTRATANTE oficiará à CONTRATADA para que esta recolha aos cofres da União, no prazo máximo de 05 dias úteis da data do recebimento do comunicado, o valor resultante dos prejuízos decorrentes da rescisão contratual ou da diferença entre estes e os créditos retidos.

14.2.2. Caso a CONTRATADA não efetue o recolhimento no prazo estipulado no subitem anterior, o valor correspondente aos prejuízos experimentados pelo CONTRATANTE será cobrado judicialmente, a critério da Administração.

CLÁUSULA DÉCIMA QUINTA - DA LICITAÇÃO

15.1. A presente contratação foi antecedida de procedimento licitatório na modalidade Pregão Eletrônico nº xx/2013, razão pela qual ficam fazendo parte integrante do ajuste, independentemente de transcrição, as disposições contidas no instrumento convocatório, bem como as condições propostas pela CONTRATADA naquilo em que não contrariarem o que aqui ficou estipulado.

15.2. Integram também o presente contrato, independentemente de transcrição, as disposições constantes da Lei nº 8.666/93, naquilo em que lhe seja aplicável.

CLÁUSULA DÉCIMA SEXTA - DA FISCALIZAÇÃO

16.1. O CONTRATANTE fiscalizará como lhe aprouver e no seu exclusivo interesse o exato cumprimento das cláusulas e condições estabelecidas neste contrato.

16.2. Caberá a Seção de Segurança de Informações e Conformidade (SESIN) do CONTRATANTE exercer a fiscalização acima estabelecida, devendo proceder a orientação, fiscalização e interdição da sua execução, se necessário, a fim de garantir o exato cumprimento das condições estabelecidas neste Contrato.

16.2.1. Será designado pela autoridade competente da administração, um Fiscal Administrativo encarregado da fiscalização do contrato quanto aos aspectos administrativos, tais como a verificação de regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.

16.3. A fiscalização da execução deste contrato por parte do CONTRATANTE não exclui nem reduz a responsabilidade da CONTRATADA em relação às obrigações por ela assumidas.

16.4. O servidor do CONTRATANTE a quem incumbir a fiscalização da execução deste contrato, terá autoridade para definir toda e qualquer ação de orientação geral, controle e acompanhamento, fixando normas nos casos não especificados e determinando as providências cabíveis.

CLÁUSULA DÉCIMA SÉTIMA - DA PUBLICAÇÃO

17.1. De conformidade com o disposto no parágrafo único do artigo 61 da Lei nº 8.666/93, o presente contrato será publicado no Diário Oficial da União, na forma de extrato.

17.2. Caberá ao CONTRATANTE promover a publicação de que trata o item 16.1 deste contrato.

CLÁUSULA DÉCIMA OITAVA - DO FORO

Para dirimir as questões oriundas do presente contrato, será competente o Juízo Federal da Seção Judiciária do Distrito Federal.

CLÁUSULA DÉCIMA NONA - DAS DISPOSIÇÕES FINAIS

19.1. Os casos omissos serão resolvidos à luz das disposições contidas na Lei nº 8.666/93, bem como dos princípios de direito público.

19.2. É defeso à CONTRATADA utilizar-se deste contrato para caucionar qualquer dívida ou títulos por ela emitidos, seja qual for a natureza dos mesmos.

19.3 A CONTRATADA assumirá, de forma exclusiva, todas as dívidas que venha a contrair com vistas a cumprir com as obrigações oriundas do presente contrato, ficando certo, desde já, que o CONTRATANTE não será responsável solidário pelas mesmas.

19.4 E para firmeza e como prova de assim haverem ajustado, foi lavrado o presente TERMO em 03 (três) vias de igual teor, uma da qual destinada à CONTRATADA, o qual, depois de lido e achado conforme, vai assinado pelos representantes das partes contratantes.

Brasília-DF, ___ de _____ de 2013.

EVA MARIA FERREIRA BARROS
Secretária-Geral do
Conselho da Justiça Federal

CONTRATADA

OBS: OS ANEXOS DO CONTRATO SERÃO OS MÓDULOS: I E SEUS ANEXOS E II DO EDITAL.

Conselho da Justiça Federal

MÓDULO IV DO PREGÃO ELETRÔNICO n. 26/2013

TERMO DE VISTORIA

Declaro que eu, _____, portador(a) do CPF(MF) nº _____, representante da empresa _____, estabelecida no endereço _____ como seu(ua) representante legal para os fins da presente declaração, tomei conhecimento, com o objetivo de participação no Pregão N._____, de todas as informações necessárias à execução dos serviços licitados e que vistoriei os locais de instalação dos equipamentos e componentes.

Brasília, ___ de _____ de 2013.

ASSINATURA DO RESPONSÁVEL TÉCNICO DA EMPRESA

NOME LEGÍVEL DO RESPONSÁVEL DA EMPRESA
NÚMERO DA CARTEIRA DE IDENTIDADE DO RESPONSÁVEL DA EMPRESA COM INDICAÇÃO DO ÓRGÃO EXPEDIDOR

RAZÃO SOCIAL DA EMPRESA:

NÚMERO DE INSCRIÇÃO NO CNPJ:

CARIMBO E ASSINATURA DO REPRESENTANTE
CONSELHO DA JUSTIÇA FEDERAL