EDITAL DO PREGÃO ELETRÔNICO N. 52/10

A COMISSÃO PERMANENTE DE LICITAÇÃO da Câmara dos Deputados, por intermédio deste Pregoeiro legalmente designado, e tendo em vista o que consta do Processo n. 105.250/09, torna pública, para conhecimento dos interessados, a abertura de licitação, na modalidade **PREGÃO ELETRÔNICO,** destinada à contratação de pessoa jurídica para prestação de serviços de implantação (licenciamento, capacitação operacional, instalação, configuração e ativação) e manutenção, que compreende garantia de funcionamento (suporte técnico) e garantia de atualização de solução de segurança de estações de trabalho (*Endpoints*) e servidores de rede pelo período de vinte e quatro meses, para a Câmara dos Deputados.

A presente licitação, do tipo "MENOR PREÇO", na forma de execução indireta sob o regime de empreitada por preço global, reger-se-á pelo disposto neste Edital e em seus Anexos, pela Portaria n. 1, de 2003, da Primeira-Secretaria da Câmara dos Deputados; pela Lei 10.520, de 2002; pela Lei Complementar n. 123, de 2006; pela Lei 8.248, de 1991, e suas alterações; pelo REGULAMENTO DOS PROCEDIMENTOS LICITATÓRIOS DA CÂMARA DOS DEPUTADOS, doravante designado como "REGULAMENTO", aprovado pelo Ato da Mesa n. 80, de 7 de junho de 2001, e publicado no Diário Oficial da União de 5 de julho de 2001, e, subsidiariamente, pela Lei 8.666, de 1993.

1. DO OBJETO DA LICITAÇÃO

1.1. O objeto do presente PREGÃO é a prestação de serviços de implantação e manutenção de solução de segurança de estações de trabalho (*Endpoints*) e servidores de rede pelo período de vinte e quatro meses.

1.1.1. Define-se implantação como licenciamento, capacitação operacional, instalação, configuração e ativação da solução de *Endpoint.*

1.1.2. Define-se manutenção como prestação de serviços de garantia de funcionamento (suporte técnico) e garantia de atualização da solução de *Endpoint*.

1.2. No interesse da Câmara dos Deputados, o valor do Contrato decorrente desta licitação poderá ser aumentado ou diminuído em até 25% (vinte e cinco por cento), em razão de acréscimos ou exclusões de componentes do objeto, nas mesmas condições contratuais da proposta, em conformidade com o parágrafo 1º do artigo 113 do REGULAMENTO.

1.2.1. As supressões além desse limite são facultadas por acordo entre as partes, em conformidade com o parágrafo 2º do artigo 113 do REGULAMENTO.

1.2.2. Os acréscimos e as exclusões de que trata este item somente serão permitidos até a entrega formal do documento contendo o Termo de Licença que

dá direito à atualização da solução de segurança de estações de trabalho (*Endpoints*) oferecida.

2. DO CRONOGRAMA DE PROCESSAMENTO DO PREGÃO

2.1. Os procedimentos básicos deste Pregão serão processados nas datas e nos horários a seguir discriminados, observado o horário oficial vigente no Distrito Federal e desta forma serão registrados no sistema eletrônico e na documentação relativa ao certame:

2.1.1. **12/3/2010:** divulgação do Pregão, mediante aviso publicado no Diário Oficial da União, no "Jornal Correio Braziliense", editados em Brasília-DF e no sítio eletrônico www.camara.gov.br na rede mundial de computadores Internet.

2.1.2. **15/3/2010:** **a partir das 9h até às 9h do dia 26/3/2010**: apresentação de propostas por meio eletrônico em formulário disponível no sítio indicado no subitem anterior.

2.1.3. **26/3/2010:** **às 9h30**: início dos procedimentos, via internet, relativos a:

a) abertura das propostas;
b) admissão das propostas formuladas em perfeita consonância com as especificações e condições previstas neste Edital;
c) divulgação do valor da proposta de menor preço, vedada a identificação da respectiva proponente;
d) abertura da etapa competitiva de lances na forma do Título 6.

2.2. Na hipótese de não haver expediente em qualquer dos dias fixados neste Edital, os eventos respectivos ficam transferidos para o primeiro dia útil subsequente, mantidos os horários preestabelecidos.

3. DA PARTICIPAÇÃO E DO CREDENCIAMENTO

3.1. O PREGOEIRO somente aceitará participação de pessoa jurídica inscrita no Cadastro de Fornecedores da Câmara dos Deputados, sendo condição essencial para a habilitação que o objetivo social, expresso no Estatuto ou Contrato Social, especifique atividade pertinente e compatível com o objeto da presente licitação, não se admitindo a apresentação de Certificado de Registro Cadastral fornecido por outro órgão.

3.2. A solicitação de Registro Cadastral deverá ser feita na Seção de Cadastro de Fornecedores da Secretaria da Comissão Permanente de Licitação da Câmara dos Deputados, localizada no Edifício Anexo I da Câmara dos Deputados, 14º andar,

sala 1406, após a formalização do pedido por meio do preenchimento do pré-cadastro na página da internet http://www2.camara.gov.br/licitacoes/fornecedores.

3.3. Por motivos operacionais, fica a Comissão Permanente de Licitação desobrigada de validar o cadastramento da pessoa jurídica cuja documentação exigida para esse fim não estiver disponibilizada na Secretaria da Comissão até dois dias úteis antes da data prevista para a abertura das propostas.

3.4. O credenciamento para participar de pregões eletrônicos dar-se-á pela atribuição de senha, pessoal e intransferível.

3.5. A senha terá validade por um ano, ressalvada a hipótese de cancelamento por iniciativa da pessoa jurídica ou por não atendimento por parte da pessoa jurídica de exigências estabelecidas pela Câmara dos Deputados.

3.6. O uso da senha de acesso é de responsabilidade exclusiva da licitante, não cabendo à Câmara dos Deputados qualquer responsabilidade por eventuais danos decorrentes de mau uso ou uso indevido.

3.7. O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante ou do seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

3.8. O interessado em participar do Pregão deverá declarar em campo próprio do sistema eletrônico que detém pleno conhecimento das exigências de habilitação previstas neste Edital e que atende às referidas exigências.

3.9. Orientações adicionais sobre como participar de pregões eletrônicos podem ser obtidas na página http://www2.camara.gov.br/licitacoes/fornecedores.

4. DO ATENDIMENTO DAS CONDIÇÕES DE HABILITAÇÃO

4.1. Serão consideradas habilitadas para o presente Pregão as licitantes que estejam inscritas no Cadastro de Fornecedores da Câmara dos Deputados, com indicação, no respectivo Certificado de Registro Cadastral, do exercício de atividade pertinente e compatível com o objeto deste Pregão e que apresentem a seguinte documentação:

4.1.1. atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado que comprove(m) que a licitante forneceu, satisfatoriamente, solução Endpoint com as funcionalidades de software antimalware; firewall pessoal; prevenção de intrusão para máquina (“Host-Based Intrusion Prevention – HIPS”) e Controle de Dispositivos (portas de comunicação) e prestou (em caso de contrato encerrado) ou esteja prestando (em caso de contrato vigente), satisfatoriamente, serviços de implantação e de suporte técnico de solução Endpoint, com indicação do número de estações de trabalho e servidores computadores protegidos pela solução *Endpoint*.

4.1.1.1. Os quantitativos mínimos exigidos serão de 1.500 (mil e quinhentas) estações de trabalho protegidas e de 20 (vinte) servidores computadores protegidos.

4.1.1.2. Devido à complexidade de planejamento, configuração e implementação dessa solução, apenas serão aceitos atestados de produtos e serviços que contenham, no mínimo, as funcionalidades descritas neste Edital.

4.1.1.3. O(s) atestado(s) dever(á)ão ser apresentado(s) em papel timbrado do cliente.

4.1.2. declaração de que possui estrutura física de suporte técnico no Brasil.

Observação: O(s) atestado(s) e a declaração deverão ser apresentados conforme modelos constantes dos Anexos n^{s}. 9 e 10 deste Edital, respectivamente.

4.2. Obriga-se a licitante a declarar, quando for o caso, sob as sanções administrativas cabíveis, a superveniência de fato impeditivo da habilitação, ou que se encontra em concordata, recuperação judicial ou estado falimentar, ou que foi declarada inidônea por qualquer órgão da Administração Pública.

4.3. A licitante deverá providenciar a inserção das cópias dos documentos referidos nos subitens 4.1.1 a 4.1.2, no documento eletrônico único a que se refere o item 5.1.

5. DAS PROPOSTAS ELETRÔNICAS

ATENÇÃO: A cotação do valor na proposta eletrônica é pelo **PREÇO TOTAL DO ITEM ÚNICO.**

5.1. Ao registrar eletronicamente o valor de sua proposta, a licitante já deverá ter pronto o conjunto de sua proposta analítica, obedecendo ao Modelo Completo da Proposta, disposto no Anexo n. 6, a documentação de habilitação (subitens 4.1.1 e 4.1.2) e a documentação técnica (Título 3 do Anexo n. 1), sendo a apresentação dessa obrigatória, configurados, preferencialmente, em documento nos seguintes formatos: Adobe Acrobat Reader (extensão .PDF) ou Word (extensão .DOC) ou Excel (extensão .XLS).

5.1.1.O conjunto da proposta analítica deverá ser disponibilizado pela ofertante do menor preço, após o término da etapa competitiva, quando solicitado pelo pregoeiro.

5.1.1.1. Simultaneamente às providências previstas no subitem 5.1.1, a licitante enviará cópia de sua proposta para o endereço eletrônico: cpl@camara.gov.br.

5.1.2. **Quando for o caso,** a licitante incluirá, no conjunto que constitui documento eletrônico referido neste item, cópia da declaração de superveniência de fato impeditivo da habilitação conforme o disposto no item 4.2 do Edital.

5.1.3. Caso não seja possível enviar, pelo sistema, a documentação de habilitação e/ou documentação técnica a que se refere o item 5.1 deste Edital, esta(s) poderá(ão) ser enviada(s) por meio do fax (0xx61) 3216-4915 ou do endereço eletrônico cpl@camara.gov.br.

5.2. A licitante implantará sua proposta eletrônica no período indicado no subitem 2.1.2 do presente Edital.

5.2.1. **Caso queira usufruir do tratamento favorecido estabelecido nos artigos 42 a 48 da Lei Complementar 123, de 2006**, a licitante enquadrada como microempresa ou empresa de pequeno porte **deverá declarar**, por ocasião do encaminhamento da proposta e em campo próprio do sistema eletrônico, que atende aos requisitos previstos no artigo 3º da referida lei.

5.2.1.1. O pregoeiro poderá solicitar documentos que comprovem o enquadramento da licitante na categoria de microempresa ou empresa de pequeno porte.

5.3. São de inteira responsabilidade da licitante todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

5.4. Incumbirá ainda à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão Eletrônico, ficando responsável pelo ônus decorrente da perda de negócios em razão de pane ou falha de seu computador ou provedor ou da inobservância de quaisquer mensagens emitidas pelo sistema ou pela desconexão.

5.5. O acesso à sessão pública do Pregão Eletrônico dar-se-á por meio da digitação do CNPJ e da senha privativa que automaticamente será associada à razão social da licitante, mantido o sigilo absoluto.

5.6. A proposta da licitante apresentada exclusivamente no sítio https://compras.camara.gov.br/compras/licitante explicitará o **preço total do item único** e as demais informações necessárias (ver Anexo n. 7).

5.7. A proposta deve contemplar todos os subitens que compõem o item único do certame, sob pena de desclassificação.

6. DA FORMULAÇÃO DE LANCES

6.1. Na data e no horário determinados para a abertura das propostas, o PREGOEIRO fará divulgar o **MENOR PREÇO TOTAL oferecido PARA O ITEM,** dando início, em seguida, à etapa competitiva.

6.2. Na etapa competitiva, as licitantes poderão oferecer lances sucessivos para o item, exclusivamente por meio do sistema eletrônico, sendo imediatamente informadas, em tempo real, do seu recebimento, do horário do registro e do valor ofertado.

6.2.1. Os lances deverão ser, necessariamente, **inferiores** ao último lance ofertado pela própria licitante.

6.3. Na hipótese de oferecimento de mais de um lance de idêntico valor, será considerado como válido, para efeito de classificação, aquele que tiver sido recebido em primeiro lugar pelo sistema eletrônico.

6.4. A duração inicial da etapa de lance será de **quinze** minutos, cujo término iminente será objeto de aviso emitido pelo sistema eletrônico, após o que transcorrerá um período adicional com duração definida aleatoriamente num intervalo de até trinta minutos, findo o qual será automática e definitivamente encerrada a recepção de lances.

6.5. Alternativamente, e a critério exclusivo do PREGOEIRO, o período adicional de que trata o item anterior poderá ser fixado em trinta minutos, mediante comunicação a ser feita no momento do aviso do término iminente do período inicial.

6.6. Só serão considerados válidos os lances que forem registrados pelo sistema eletrônico até o exato momento determinado para o encerramento da recepção desses.

6.7. Após a fase de lances, verificando-se que a **proposta mais bem classificada não** é de licitante enquadrada como microempresa ou empresa de pequeno porte e **existindo proposta de empresa que fez a declaração prevista no subitem 5.2.1 deste Edital**, será observado o seguinte:

6.7.1. O sistema, de forma automática, verificará a ocorrência de empate, nos termos do art. 44 da Lei Complementar n. 123, de 2006, assegurando, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte.

6.7.1.1. Entende-se por empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à melhor proposta.

6.7.2. Verificado o empate, a microempresa ou empresa de pequeno porte mais bem classificada poderá, **no prazo preclusivo de 5 (cinco) minutos, contados do envio de mensagem pelo sistema,** apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que será adjudicado em seu favor o objeto licitado.

6.7.2.1. A adjudicação fica condicionada ao atendimento do disposto no Título 9 deste Edital.

6.7.3. Não ocorrendo a contratação da microempresa ou empresa de pequeno porte mais bem classificada na forma do subitem 6.7.2, serão convocadas as remanescentes que porventura se enquadrem na hipótese do subitem 6.7.1.1, na ordem classificatória, para o exercício do mesmo direito.

6.7.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem no intervalo estabelecido no subitem 6.7.1.1, o sistema fará um sorteio eletrônico, definindo automaticamente a vencedora para o encaminhamento da oferta final do desempate, conforme inciso III do art. 45 da Lei Complementar 123, de 2006.

6.7.5. Na hipótese da não-contratação nos termos previstos no caput do artigo 45 da Lei Complementar n. 123, de 2006, o objeto licitado será adjudicado em favor da proposta originalmente mais bem classificada.

6.8. Se não ocorrer a hipótese prevista no item 6.7 deste Edital e for verificado empate nominal entre duas ou mais propostas após a fase de lances, será dada preferência à licitante que comprovar que os bens ou serviços foram desenvolvidos com tecnologia nacional e cumpriram com o processo produtivo básico, nos termos do art. 3º da Lei 8.248, de 1991.

6.8.1. Persistindo o empate, a classificação observará o disposto no § 2º do art. 45 da Lei 8.666, de 1993.

6.9. Após a etapa competitiva, o PREGOEIRO poderá encaminhar à licitante que tenha apresentado a proposta ou o lance de menor valor, contraproposta visando à obtenção de preço melhor.

6.10. Se decidir pela aceitação do preço ofertado, o PREGOEIRO, após a conclusão da etapa competitiva, anunciará aos participantes o resultado, informando o nome da ofertante do menor preço e procederá à verificação do atendimento das condições de habilitação por parte dessa proponente.

6.11. Não será considerada qualquer oferta de vantagem não prevista neste Edital, sendo ainda desclassificada a proposta ou lance que consignar preços unitários ou total excessivos, manifestamente inexequíveis, simbólicos, irrisórios ou de valor zero.

6.11.1. Entende-se por preço unitário ou total excessivo aquele que, após a fase de lances ou negociação, extrapolar os valores apresentados no orçamento estimado constante do Anexo n. 14 deste Edital.

6.11.2. Os preços unitário e total referentes ao subitem 1.5 do objeto da licitação contido no Anexo n. 1 (Funcionalidade de proteção contra códigos maliciosos no Exchange Server 2003) constantes do Anexo n. 14 deste Edital não serão considerados como preços máximos, **uma vez que essa funcionalidade poderá ser cotada por caixas postais eletrônicas ou por computadores servidores**.

6.12. No caso de não aceitação do lance de menor valor, o PREGOEIRO examinará a proposta ou lance imediatamente subsequente, procedendo na forma do item 6.7.

6.13. Durante a fase de lances, o Pregoeiro poderá excluir, justificadamente, lance cujo valor for considerado inexequível.

6.14. Não será admitida desistência de lances ofertados, sujeitando-se a licitante às sanções administrativas constantes do item 12.1.

7. DA PROPOSTA ANALÍTICA

ATENÇÃO: A proposta analítica só será enviada pelo autor da proposta de menor preço. Faça o download do modelo em http://www2.camara.gov.br/licitacoes/editais/pregaoeletronico.html.

7.1. É **obrigatório** que a proposta analítica seja elaborada na forma do "Modelo Completo da Proposta" constante do Anexo n. 6, dispensada qualquer outra informação adicional não expressamente exigida.

7.2. A proposta será apresentada preferencialmente em duas vias, sem emendas, rasuras ou entrelinhas, datada, assinada por quem de direito, e deverá explicitar:

a) nome, CNPJ, endereço, fone/fax e endereço eletrônico da licitante;
b) menção a este Pregão, com indicação do seu número;
c) prazo de validade da proposta de, no mínimo, sessenta dias, contados da data prevista para abertura da licitação;
d) prazos de entrega dos componentes e conclusão dos serviços de configuração e ativação da solução; distribuição das funcionalidades configuradas nos equipamentos em rede; bem como de capacitação operacional, conforme Cronograma de Encadeamento das Fases disposto no Título 3 do Anexo n. 4;
e) prazos de garantia de funcionamento e atualização referentes:
    e.1) aos subitens 1.1 a 1.5 do objeto da licitação contido no Anexo n. 1 de, no mínimo, vinte e quatro meses, contados do Recebimento Provisório da Solução (após a conclusão da Fase 3 do Cronograma de Encadeamento das Fases - Anexo n. 4);
    e.2) ao subitem 1.9 do objeto da licitação contido no Anexo n. 1 de, no mínimo, vinte e um meses, contados da data do Recebimento Definitivo da Solução (após a conclusão da Fase 4 do Cronograma de Encadeamento das Fases - Anexo n. 4);
f) indicação dos componentes oferecidos e dos serviços a serem executados, em conformidade com a descrição contida nos Anexos n^{s}. 1 e 2, com informação das marcas, dos modelos, dos tipos, do pacote, dos componentes e subcomponentes e quaisquer outras informações aplicáveis e necessárias à perfeita caracterização dos produtos e serviços ofertados, de forma a permitir a correta identificação destes, na documentação técnica apresentada;
    f.1) a indicação de marca deve ser precisa, **vedada** a aposição de referências genéricas como "ou similar" e outras;
g) detalhamento da forma de licenciamento de cada componente da solução de segurança das estações de trabalho (Endpoints) e servidores de rede;
h) preços unitário e total por subitem (em algarismos) e preço total do item único (em algarismos e por extenso), neles incluídos todos os custos e todas as despesas, diretas e indiretas, para o licenciamento

da solução de segurança e a execução dos serviços objeto da presente licitação, em conformidade com as especificações constantes do Anexo n. 2, para a Câmara dos Deputados, em Brasília, DF;

h.1) ocorrendo divergência entre o preço expresso em algarismos e o por extenso, prevalecerá este último;

i) declaração da licitante, integrante da proposta, de que conhece a natureza e as condições de execução dos serviços referentes ao objeto desta licitação, observado o disposto no Título 4 do Anexo n. 1.

8.DA VERIFICAÇÃO DAS CONDIÇÕES DE HABILITAÇÃO

8.1. O PREGOEIRO considerará preliminarmente aceita a proposta de menor preço se comprovado o exercício de atividade pertinente e compatível com o objeto da licitação, mediante consulta ao Cadastro de Fornecedores da Câmara.

8.2. Manifestada a aceitação de que trata o item anterior, a ofertante do menor preço deverá apresentar imediatamente o conteúdo integral de sua proposta no campo que lhe será disponibilizado para tal no sítio em que se realiza o pregão, bem como os documentos condicionantes para classificação ou habilitação exigidos no Edital.

8.2.1. O conteúdo da proposta deve corresponder à oferta final da licitante no valor correspondente ao lance final.

8.2.2. O não atendimento das disposições deste item, sem justificativa aceita pelo PREGOEIRO implicará a desclassificação da proposta ofertada.

8.3. O conteúdo da proposta de menor preço será disponibilizado eletronicamente aos participantes.

8.4. No prazo de até setenta e duas horas, contadas do momento da divulgação de que trata o item anterior, a licitante vencedora deverá entregar na Secretaria da Comissão Permanente de Licitação da Câmara dos Deputados, localizada no Edifício Anexo I da Câmara dos Deputados, 14º andar, sala 1406, CEP: 70160.900, os originais da proposta analítica e dos demais documentos ou suas cópias devidamente autenticadas, feitos os ajustes cabíveis em relação aos valores finais decorrentes da oferta de lances ou de negociação.

8.5. Caso não tenham sido atendidas as exigências para habilitação, o PREGOEIRO declarará a licitante inabilitada e convocará a autora do menor preço subsequente, repetindo os procedimentos, até que se logre a habilitação de licitante que tenha atendido todas as exigências para essa finalidade.

8.6. Caso todas as licitantes que oferecerem lances venham a ser inabilitadas ou desclassificadas o PREGOEIRO poderá, a seu critério, promover nova sessão de lances, considerado o menor preço apresentado pelas licitantes remanescentes.

9. DA ADJUDICAÇÃO

9.1. O PREGOEIRO anunciará como vencedora a licitante habilitada, devidamente nominada, que tiver oferecido o **menor preço total PARA O ITEM LICITADO** e houver sido classificada em razão do atendimento às disposições do item 8.2 e,

ainda, **após comprovação das características da solução oferecida, mediante realização da Prova de Conceito, em conformidade com o Anexo n. 11 deste Edital.**

9.1.1. O órgão fiscalizador elaborará ata circunstanciada dos testes executados, dos resultados obtidos e um parecer final sobre a solução avaliada.

9.2. Durante trinta minutos, contados do momento da divulgação de que trata o item anterior, as licitantes poderão manifestar-se pela intenção de interpor recurso contra a decisão do PREGOEIRO, apresentando na forma disponibilizada no sistema eletrônico, de modo objetivo e conciso, os motivos da contestação.

9.3. A falta de manifestação imediata e motivada pela interposição de recurso importará a decadência do direito de recorrer.

9.4. Em caso de não ser aceita a manifestação de que trata o item 9.2, por falta de fundamentação, ou se não ocorrerem manifestações formais no sentido de interpor recurso, o PREGOEIRO adjudicará o objeto do Pregão à licitante vencedora.

9.5. O ato de adjudicação do objeto do procedimento licitatório pelo PREGOEIRO ficará sujeita à homologação do Diretor-Geral da Câmara dos Deputados.

10. DO RECURSO, DA IMPUGNAÇÃO CONTRA ATOS DO PREGOEIRO E DAS CONSULTAS

10.1. Às licitantes que tenham se manifestado no prazo concedido na forma do item 9.2, será concedido o prazo de três dias para apresentação, preferencialmente, por via eletrônica, das razões do recurso, ficando as demais licitantes desde logo intimadas para apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos autos.

10.1.1. Os autos do processo permanecerão com vista franqueada às interessadas na Secretaria da Comissão Permanente de Licitação, localizada no Edifício Anexo I da Câmara dos Deputados, 14° andar, sala 1407.

10.1.2. Na impossibilidade do envio eletrônico das razões do recurso, a recorrente poderá encaminhar o respectivo documento por meio do fax (61) 3216-4915 ou entregá-lo no endereço citado no subitem anterior.

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

10.3. Até dois dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa poderá impugnar o ato convocatório do Pregão, por meio do endereço eletrônico cpl@camara.gov.br ou pelo fax (0xx61) 3216-4915.

10.3.1. Caberá ao PREGOEIRO decidir sobre a petição, no prazo de vinte e quatro horas, contados de seu recebimento.

10.3.2. Acolhida a petição contra o ato convocatório, caso advenha eventual modificação do edital que afete a formulação das propostas, será designada nova data para a realização do certame.

10.4. Os pedidos de esclarecimentos referentes ao pregão deverão ser encaminhados ao pregoeiro até três dias úteis anteriores à data fixada no subitem 2.1.3, por meio do endereço eletrônico: cpl@camara.gov.br ou pelo fax (61) 3216-4915.

10.4.1. A síntese das consultas e das respostas dadas, omitido o nome da consultante, será disponibilizada no campo "Esclarecimentos", da página: http://www2.camara.gov.br/licitacoes/editais/pregaoeletronico.html.

11. DAS OBRIGAÇÕES DA EXECUTANTE DOS SERVIÇOS

11.1. A adjudicatária do presente Pregão assinará o respectivo contrato no prazo de cinco dias úteis a partir da sua notificação.

11.1.1. O prazo para assinatura do Contrato poderá ser prorrogado uma única vez, por igual período, quando solicitado pela adjudicatária durante o seu transcurso, e desde que ocorra motivo justificado e aceito pela Câmara.

11.1.2. O Contrato terá vigência a partir da data de sua assinatura até o término do prazo de garantia de funcionamento e atualização da solução, obedecido ao disposto no item 7.2 do Edital, admitida a prorrogação para a prestação dos serviços de suporte técnico e atualização, em conformidade com o inciso II do Artigo 57 da Lei 8.666, de 1993, e com o inciso II do Artigo 105 do REGULAMENTO, a critério da Câmara dos Deputados.

11.1.3. Para a assinatura do contrato, a adjudicatária fornecerá ao órgão fiscalizador o nome de seu preposto ou empregado com competência para manter entendimentos e receber comunicações ou transmiti-las ao órgão incumbido da fiscalização do contrato.

11.2. Além do estatuído neste Edital e em seus Anexos, a contratada cumprirá as instruções complementares do órgão fiscalizador, quanto à execução e ao horário de realização dos serviços, permanência e circulação de pessoas nos prédios administrativos da Câmara dos Deputados.

11.2.1. Para o pessoal em serviço será exigido o porte de cartão de identificação, a ser fornecido pela prestadora dos serviços ou, no interesse administrativo, pelo Departamento de Polícia Legislativa.

11.2.2. A Câmara dos Deputados poderá, de forma fundamentada, solicitar à contratada que substitua os profissionais empregados que não estejam cumprindo a contento as atividades que lhes foram confiadas, devendo os substitutos possuírem as qualificações exigidas para a prestação do serviço.

11.2.2.1. O empregado acima referido deve ser substituído pela contratada no prazo máximo de 15 (quinze) dias.

11.3. A contratada assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da Câmara dos Deputados ou de terceiros por ação ou omissão de seus empregados ou prepostos, na área de prestação dos serviços, mesmo que fora do exercício das atribuições previstas no contrato.

11.4. A contratada comunicará, verbal e imediatamente, ao órgão fiscalizador, todas as ocorrências anormais verificadas na execução dos serviços e, **em até cinco dias após o ocorrido**, reduzirá a escrito a comunicação verbal, acrescentando todos os dados e circunstâncias julgados necessários ao esclarecimento dos fatos.

11.5. Os empregados da contratada, por esta alocados na execução dos serviços, embora sujeitos às normas disciplinares ou convencionais da Casa, não terão com ela qualquer vínculo empregatício.

11.5.1. Todas as obrigações tributárias, trabalhistas e sociais da contratada e de seus empregados serão de inteira responsabilidade desta.

11.6. A contratada ficará obrigada a reparar, corrigir, refazer ou substituir, a suas expensas, no todo ou em parte, o objeto do contrato em que se verificarem imperfeições, vícios, defeitos ou incorreções resultantes da execução dos serviços ou de materiais empregados, por exigência do órgão fiscalizador, que lhe assinará prazo compatível com as providências ou reparos a realizar.

11.7. A contratada deverá marcar, por meio do telefone (61) 3216-3793 ou email seseg.cenin@camara.gov.br, uma reunião preparatória que deverá ocorrer dentro do prazo de três dias, contados da data de assinatura do contrato, que tratará, dentre outros assuntos pertinentes, do cronograma de execução da capacitação operacional, do cronograma de implantação da solução e do modo de abertura de chamados técnicos.

11.7.1. Na reunião preparatória deverá ser indicado ao menos um técnico com certificação na solução ofertada, com apresentação de documentação que comprove a certificação exigida e, ainda, documentação que comprove o vínculo do(s) profissional(ais) indicado(s), com a contratada. A indicação do técnico e sua documentação deverão ser aprovados formamente pelo órgão fiscalizador.

11.7.1.1 A comprovação do vínculo do(s) profissional(ais) indicado(s) no subitem 11.7.1 com a contratada se dará por meio da apresentação de original ou cópia autenticada de:

a) CTPS ou registro de empregado, quando o vínculo for de natureza trabalhista;
b) estatuto ou contrato social, quando o vínculo for societário;
c) contrato de prestação de serviços, regido pela legislação civil, quando o vínculo for contratual.

11.8. O objeto contratual será recebido em quatro fases distintas, conforme Cronograma disposto no Título 3 do Anexo n. 4 deste Edital, se em perfeitas

condições e conforme as especificações editalícias a que se vincula a proposta da Contratada.

11.8.1. O Recebimento Provisório da Solução se dará após a conclusão e o aceite da Fase 3 e o Recebimento Definitivo da Solução se dará após a conclusão e o aceite da Fase 4, **observado o disposto no Título 1 do Anexo n. 4 deste Edital**.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1. A licitante que deixar de entregar a documentação exigida para o certame, apresentar documentação falsa, ensejar o retardamento da execução do objeto da licitação, não mantiver a proposta, faltar ou fraudar com suas obrigações estipuladas neste Edital e no contrato, comportar-se de modo inidôneo ou cometer fraude fiscal ficará impedida de licitar e contratar com a Câmara dos Deputados pelo prazo de até cinco anos, sem prejuízo de multas previstas no Edital e das demais cominações legais.

12.1.1. Pelo descumprimento de outras obrigações assumidas, considerada a gravidade da transgressão, serão aplicadas as sanções previstas no art. 87 da Lei 8.666, de 1993, a saber:

a) advertência, formalizada por escrito;
b) multa, nos casos previstos neste Edital;
c) suspensão temporária para licitar e impedimento para contratar com a Câmara dos Deputados;
d) declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, nos termos da lei.

12.2. Caso a adjudicatária não assine o contrato no prazo fixado no item 11.1 deste Edital, sem justificativa ou com justificativa não aceita pela Câmara dos Deputados, caracterizar-se-á o descumprimento total da obrigação assumida.

12.2.1. Ocorrendo a hipótese referida neste item, a Câmara dos Deputados anulará a Nota de Empenho e aplicará à adjudicatária multa de até 10% (dez por cento) do valor total da adjudicação, instaurando processo para apuração de responsabilidade, do qual poderão resultar a suspensão do direito de participar de licitação e o impedimento de contratar com a Câmara dos Deputados pelo prazo de até cinco anos.

12.2.2. Se a adjudicatária for reincidente, além da multa de 10% (dez por cento) do valor da adjudicação, ser-lhe-á cominada a sanção administrativa de suspensão do direito de participar de licitação e contratar com a Câmara dos Deputados pelo prazo de cinco anos.

12.3. Caso a adjudicatária não assine o contrato no prazo fixado no item 11.1 deste Edital, a Câmara dos Deputados reserva-se o direito de convocar outra licitante, observada a ordem de classificação, para fazê-lo em conformidade com a sua proposta, e assim sucessivamente, sem prejuízo das sanções cabíveis.

12.4. Ocorrendo atraso injustificado ou com justificativa não aceita pela Câmara dos Deputados na realização da Reunião Preparatória à contratada será imposta multa calculada sobre o somatório dos valores dos subitens 1.1 a 1.5 do item único do objeto da licitação contido no Anexo n. 1, de acordo com a seguinte tabela:

DIAS DE ATRASO	ÍNDICE DE MULTA	DIAS DE ATRASO	ÍNDICE DE MULTA	DIAS DE ATRASO	ÍNDICE DE MULTA
1	0,1%	**15**	2,0%	**29**	5,7%
2	0,2%	**16**	2,2%	**30**	6,0%
3	0,3%	**17**	2,4%	**31**	6,4%
4	0,4%	**18**	2,6%	**32**	6,8%
5	0,5%	**19**	2,8%	**33**	7,2%
6	0,6%	**20**	3,0%	**34**	7,6%
7	0,7%	**21**	3,3%	**35**	8,0%
8	0,8%	**22**	3,6%	**36**	8,4%
9	0,9%	**23**	3,9%	**37**	8,8%
10	1,0%	**24**	4,2%	**38**	9,2%
11	1,2%	**25**	4,5%	**39**	9,6%
12	1,4%	**26**	4,8%	**40**	10,0%
13	1,6%	**27**	5,1%		
14	1,8%	**28**	5,4%		

12.5. Não será aplicada multa de valor igual ou inferior a 10% da quantia definida na Portaria n. 49, de 1º de abril de 2004, do Ministério da Fazenda, ou em norma que vier a substituí-la, para inscrição de débito na Dívida Ativa da União.

12.5.1. Não se aplica o disposto neste item, quando verificada, num período de 60 (sessenta) dias, a ocorrência de multas que somadas ultrapassem o valor fixado para inscrição em Dívida Ativa.

12.6. Findo o prazo fixado, sem que a contratada tenha realizado a Reunião Preparatória, além da multa prevista no item 12.4, poderá, a critério da Câmara dos Deputados, ser cancelada, parcial ou totalmente, a Nota de Empenho, sem prejuízo de outras sanções legais cabíveis.

12.7. Se a contratada, a qualquer tempo, deixar de executar os serviços ficará sujeita à multa de até 10% (dez por cento) sobre o valor remanescente do contrato, sem prejuízo de outras sanções legais cabíveis.

12.8. Os valores relativos a multas aplicadas e a danos e prejuízos eventualmente causados serão descontados dos pagamentos devidos pela Câmara dos Deputados ou recolhidos pela contratada à Coordenação de Movimentação Financeira, dentro de cinco dias úteis, a partir da sua notificação por carta, ou ainda, cobrados na forma da legislação em vigor, independentemente de qualquer procedimento judicial ou extrajudicial.

12.9. O contrato poderá ser rescindido nas hipóteses aventadas pelo artigo 126 do REGULAMENTO.

12.10. Ocorrendo rescisão contratual na forma do inciso I do artigo 127 do REGULAMENTO, a Câmara dos Deputados adotará as medidas ordenadas pelo artigo 128 do citado ato normativo.

12.11. A aplicação de multas, sanção administrativa, não reduz nem isenta a obrigação da contratada de ressarcir integralmente eventuais danos causados à Administração.

12.12. Pelo não cumprimento das obrigações contratuais, ou execução insatisfatória dos serviços, omissão e outras faltas não justificadas ou se a Câmara dos Deputados julgar as justificativas improcedentes, poderão ser impostas à contratada multas por infração cometida, de acordo com a tabela constante do Anexo n. 8 deste Edital, limitadas, em qualquer caso, a 10% (dez por cento) do valor do contrato, observado o disposto no item 12.8.

13. DO PAGAMENTO

13.1. O pagamento dos **subitens 1.1 a 1.7, 1.9 e 1.10** do objeto da licitação contido no Anexo n. 1, referentes à entrega dos componentes, realização da capacitação operacional, configuração e ativação da solução, distribuição das funcionalidades configuradas nos equipamentos em rede para a Câmara dos Deputados e por esta aceitos, será feito de acordo com o Cronograma de Encadeamento das Fases disposto no Título 3 do Anexo n. 4, por meio de depósito em conta corrente da contratada, em agência bancária indicada, mediante a apresentação, em duas vias, de nota fiscal/fatura discriminada, após emissão do Aceite Provisório ou Definitivo, conforme o caso, pelo órgão fiscalizador.

13.2. O pagamento dos serviços referentes à garantia de funcionamento (suporte técnico) e atualização da solução se dará conforme abaixo:

13.2.1. Os serviços referentes ao **subitem 1.8 do objeto da licitação** contido no Anexo n. 1 executados pela contratada e aceitos pela Câmara dos Deputados será efetuado em vinte e quatro parcelas mensais, após o primeiro mês de prestação dos referidos serviços, que terão início a partir da data do Recebimento Provisório da Solução – (após a conclusão da Fase 3 do Cronograma de Encadeamento das Fases), não se admitindo o pagamento antecipado sob qualquer pretexto.

13.2.2. Os serviços referentes ao **subitem 1.11 do objeto da licitação** contido no Anexo n. 1 executados pela contratada e aceitos pela Câmara dos Deputados será efetuado em vinte e uma parcelas mensais, após o primeiro mês de prestação dos referidos serviços, que terão início a partir da data do Recebimento Definitivo da Solução (após a conclusão da Fase 4 do Cronograma de Encadeamento das Fases), não se admitindo o pagamento antecipado sob qualquer pretexto.

13.2.3. O pagamento de cada parcela será feito por meio de depósito em conta corrente da contratada, em agência bancária indicada, mediante a apresentação em duas vias de nota fiscal/fatura discriminada, emitida no

mês subsequente ao da prestação dos serviços, após atestação pelo órgão fiscalizador.

13.3. A instituição bancária, a agência e o número da conta deverão ser mencionados na nota fiscal/fatura.

13.4. A nota fiscal/fatura deverá ser acompanhada da Certidão Negativa de Débitos para com o INSS – CND, e do Certificado de Regularidade do FGTS – CRF, ambos dentro do prazo de validade neles expresso.

13.5. O pagamento será feito com prazo não superior a trinta dias, contados a partir do aceite dos serviços e da comprovação da regularidade da documentação fiscal apresentada, prevalecendo a data que ocorrer por último.

13.5.1. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela Contratante, entre a data referida no *caput* deste item e a correspondente ao efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, são calculados por meio da aplicação da seguinte fórmula:

$$\mathbf{EM = I \times N \times VP}$$

Na qual:
EM = Encargos Moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso;
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = \frac{i}{365} \qquad I = \frac{6/100}{365} \qquad I = 0{,}00016438$$

em que *i* = taxa percentual anual no valor de 6%.

13.6. Quando aplicável, o pagamento efetuado pela Câmara dos Deputados estará sujeito às retenções de que tratam o art. 31 da Lei 8.212, de 1991, com redação dada pelas Leis 9.711, de 1998 e 11.488, de 2007, além das previstas no art. 64 da Lei 9.430, de 1996 e demais dispositivos legais que obriguem a retenção de tributos.

13.7. Estando a contratada isenta das retenções referidas no item anterior, a comprovação deverá ser anexada à respectiva fatura.

14. DA DOTAÇÃO

14.1. A despesa relativa ao objeto deste Pregão correrá à conta da seguinte classificação orçamentária:

Programas de Trabalho:

01.031.0553.4061.0001 – Processo Legislativo e

01.128.0553.4091.0001 – Capacitação de Recursos Humanos

Naturezas da Despesa
3.0.00.00 - DESPESAS CORRENTES
3.3.00.00 - OUTRAS DESPESAS CORRENTES
3.3.90.00 - APLICAÇÕES DIRETAS
3.3.90.39 - Outros Serviços de Terceiros (Pessoa Jurídica)
e

4.0.00.00 - DESPESAS DE CAPITAL
4.4.00.00 - INVESTIMENTOS
4.4.90.00 - APLICAÇÕES DIRETAS
4.4.90.39 - Outros Serviços de Terceiros (Pessoa Jurídica)

15. DAS DISPOSIÇÕES GERAIS

15.1. Constituem anexos do Edital, dele fazendo parte integrante:

a). Anexo n. 1 – Demais Disposições Gerais;
b). Anexo n. 2 – Especificações Técnicas;
c). Anexo n. 3 – Capacitação Operacional;
d). Anexo n. 4 – Instalação da Solução e Cronograma de Encadeamento das Fases;
e). Anexo n. 5 – Serviços de Suporte Técnico e Atualização;
f). Anexo n. 6 – Modelo Completo da Proposta;
g). Anexo n. 7 – Cópia do Formulário Eletrônico de Entrada dos Dados da Proposta;
h). Anexo n. 8 – Tabela de Multas;
i). Anexo n. 9 – Modelo de Atestado de Capacidade Técnica;
j). Anexo n. 10 – Modelos de Declaração de Estrutura Física de Suporte Técnico e de Avaliação de Capacitação Operacional;
k). Anexo n. 11 – Prova de Conceito;
l). Anexo n. 12 – Modelo do Termo de Confidencialidade;
m). Anexo n. 13 – Glossário;
n). Anexo n. 14 – Orçamento Estimado;
o). Anexo n. 15 – Minuta do Contrato.

15.2. O presente Pregão poderá ser transferido, a critério da Câmara dos Deputados, revogado, por interesse público, ou anulado, em caso de ilegalidade, sem que, por quaisquer desses motivos, possam as interessadas reclamar direitos, observado o disposto nos parágrafos do artigo 91 do REGULAMENTO.

15.3. A Câmara dos Deputados, assegurado o direito de defesa, por despacho fundamentado de seu Diretor-Geral, poderá desclassificar licitante, sem que a esta caiba o direito de reclamar qualquer indenização e sem prejuízo de outras sanções, se lhe chegar ao conhecimento qualquer fato ou circunstância, anterior ou posterior

ao julgamento desta licitação, que desabone ou infirme a idoneidade, a capacidade jurídica, financeira ou técnica da participante.

15.4. É facultado ao PREGOEIRO ou à autoridade superior, em qualquer fase da licitação, promover diligência destinada a esclarecer ou complementar a instrução do processo.

15.5. Os prazos referidos neste Edital e em seus Anexos somente começam a fluir a partir da intimação formal realizada pela Câmara dos Deputados ou do termo inicial preestabelecido.

15.5.1. Consideram-se feitas as intimações, convocações ou comunicações dos participantes na própria sessão pública do Pregão Eletrônico ou pela publicação dos atos no Diário Oficial da União ou, quando previstas, por carta.

15.5.2. Só se iniciam e vencem os prazos em dia de expediente normal da Câmara dos Deputados.

15.5.3. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento.

15.6. Os casos omissos e as dúvidas suscitadas em qualquer fase do presente Pregão serão resolvidos pelo PREGOEIRO.

15.7. Fica eleito o foro da Justiça Federal em Brasília, Distrito Federal, para decidir demandas judiciais decorrentes deste procedimento licitatório.

15.8. Durante a execução contratual, sendo a contratada objeto de fusão, incorporação ou cisão, a Câmara dos Deputados examinará a conveniência de manter em vigência o Contrato celebrado.

15.8.1. A manutenção da vigência contratual dependerá, em qualquer caso, do atendimento pela nova sociedade empresária das condições de habilitação consignadas neste edital e de não serem alteradas as condições de execução do Contrato.

15.9. Cópia deste Edital e de seus Anexos poderá ser obtida no sítio eletrônico www.camara.gov.br na rede mundial de computadores Internet ou mediante a apresentação da Guia de Recolhimento da União – GRU (Simples), instituída pela Instrução Normativa STN n. 3/2004, na importância de R$ 5,00 (cinco reais) em favor do Fundo Rotativo da Câmara dos Deputados, a ser entregue na Secretaria da COMISSÃO, localizada no 14º andar do Edifício Anexo I, sala 1406, nos dias úteis, das 9 às 12 horas e das 14 às 18 horas, local onde também serão prestados esclarecimentos sobre a licitação, pessoalmente ou pelos telefones:

a) **(0xx61) 3216-4920 ou 4921**: em caso de informações adicionais sobre o cadastro de fornecedor mencionado no item 3.1 deste Edital;

b) **(0xx61) 3216-4911**: nos demais casos de pedidos de esclarecimentos.

15.9.1. O recolhimento efetuado pela GRU deverá ser feito nos terminais de auto atendimento do Banco do Brasil e na página da Internet, ambos por meio da opção "pagamentos c/ código de barras – Água/Luz/Telefone/Gás", ou diretamente nos caixas daquela instituição financeira.

15.9.2. A mencionada guia deverá ser impressa pelos depositantes/recolhedores mediante acesso à Internet na página do Tesouro Nacional, no endereço

www.stn.fazenda.gov.br, clicando inicialmente no *banner* "PORTAL SIAFI" (figura localizada na coluna à direita da página), em seguida, no menu principal "Guia de Recolhimento da União" (localizado à esquerda da página) e, finalmente, no *link* "Impressão GRU-Simples" (localizado logo abaixo da opção anterior). Após o preenchimento da tela clicar em "Emitir GRU Simples".

15.9.3. Quando do preenchimento da GRU - Simples, informar nos campos:

a) Unidade Favorecida (Código): 010090, Gestão: 00001;
b) Recolhimento (Código): 28830-6;
c) Número de Referência: 422.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 1

PREGÃO ELETRÔNICO N. 52/10

DEMAIS DISPOSIÇÕES GERAIS

1-DO OBJETO DA LICITAÇÃO

Item Único - Licenciamento, instalação, configuração, ativação e garantia de funcionamento e atualização de solução de segurança de estações de trabalho (Endpoints) e servidores de rede, incluindo capacitação operacional.

Subitem 1.1 - Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)
CARACTERÍSTICAS: Componente da solução integrada de software para proteção de estações e servidores de rede contra código malicioso (malware).
O software deverá ter licença definitiva, por tempo indeterminado e sem limitações, em nome da Câmara dos Deputados.
Unidade: LICENÇA
Quantidade: 1800

Subitem 1.2 - Funcionalidade de controle de acesso à rede local de computadores
CARACTERÍSTICA(S):Componente da solução integrada de software para proteção de estações e servidores de rede contra código malicioso (malware).
O software deverá ter licença definitiva, por tempo indeterminado e sem limitações, em nome da Câmara dos Deputados.
Unidade: LICENÇA
Quantidade: 7500

Subitem 1.3 - Funcionalidade de criptografia de discos rígidos de estações de trabalho
CARACTERÍSTICA(S):Componente da solução integrada de software para proteção de estações e servidores de rede contra acesso indevido.
O software deverá ter licença definitiva, por tempo indeterminado e sem limitações, em nome da Câmara dos Deputados.
Unidade: LICENÇA
Quantidade: 600

Subitem 1.4 - Funcionalidade de controle de acesso de dispositivos às portas de comunicação de estações e servidores de rede
CARACTERÍSTICA(S):Componente da solução integrada de software para proteção de estações e servidores de rede contra código malicioso (malware).
O software deverá ter licença definitiva, por tempo indeterminado e sem limitações, em nome da Câmara dos Deputados.
Unidade: LICENÇA
Quantidade: 7700

Subitem 1.5 - Funcionalidade de proteção contra códigos maliciosos no Exchange Server 2003
CARACTERÍSTICA(S):Antimalware para Exchange Server 2003 para proteção de **12.100 (doze mil e cem) caixas postais eletrônicas OU para 6 (seis) computadores servidores executando Exchange Server 2003.**
O software deverá ter licença definitiva, por tempo indeterminado e sem limitações, em nome da Câmara dos Deputados.
Unidade: SERVIÇO
Quantidade: 1

Subitem 1.6 - Instalação e configuração (Subitens 1.1 a 1.5)
CARACTERÍSTICAS DO SERVIÇO: Serviços de instalação e configuração.
Unidade: SERVIÇO
Quantidade: 1

Subitem 1.7 - Capacitação operacional
SERVIÇOS: Capacitação operacional para cinco servidores da Câmara dos Deputados na utilização da solução Endpoint.
CARACTERÍSTICA(S): A capacitação dos usuários compreende a execução de cursos específicos e suficientes para a plena operação do produto pelos usuários nomeados pelo Centro de Informática, conforme conteúdo programático original e material didático homologado pelo seu fabricante.
Unidade: SERVIÇO
Quantidade: 1

Subitem 1.8 - Garantia de funcionamento e de atualização da solução por vinte e quatro meses (Subitens 1.1 a 1.5)
SERVIÇOS: Suporte Técnico e de Atualização da Solução por um período de 24 (vinte e quatro) meses.
Unidade: serviço
Quantidade: 1

Subitem 1.9 - Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)
CARACTERÍSTICAS: Componente da solução integrada de software para proteção de estações e servidores de rede contra código malicioso (malware).
O software deverá ter licença definitiva, por tempo indeterminado e sem limitações, em nome da Câmara dos Deputados.
Unidade: LICENÇA
Quantidade: 5.900

Subitem 1.10 - Instalação e configuração (Subitem 1.9)
CARACTERÍSTICAS DO SERVIÇO: Serviços de instalação e configuração de 5.900 licenças de uso da funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)
Unidade: SERVIÇO
Quantidade: 1

Subitem 1.11 - Garantia de funcionamento e de atualização por vinte e um meses (Subitem 1.9)
SERVIÇOS: Suporte Técnico e de Atualização da Solução por um período de 21 (vinte e um) meses para 5.900 licenças de uso da funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS).
Unidade: serviço
Quantidade: 1

2-DAS ESPECIFICAÇÕES

As especificações são as descritas no Anexo n. 2 – Especificações Técnicas.

3-DA COMPROVAÇÃO DAS CARACTERÍSTICAS TÉCNICAS

3.1- O atendimento às características técnicas deverá ser comprovado mediante catálogos, publicações originais do fabricante (manuais impressos ou mídia eletrônica), impressão de relatórios gerados pela solução *Endpoint* ofertada, impressão das páginas do sítio Internet do fabricante ou das telas de gerenciamento do produto, passíveis de confirmação a qualquer momento.

3.2- A licitante deverá preencher a tabela de indicação da documentação técnica e das páginas que comprovam a conformidade da solução proposta com as especificações técnicas constantes do Anexo n. 2 deste Edital. A proposta poderá ser desclassificada caso a documentação apresentada não seja suficientemente clara, contendo, por exemplo, procedimentos passo a passo de configuração, para comprovar o atendimento dos requisitos técnicos.

4-DA VISTORIA TÉCNICA

4.1– Durante o prazo de elaboração de propostas, ficarão disponíveis os equipamentos, a rede, as instalações e o ambiente da Câmara dos Deputados, referentes aos serviços objeto desta licitação, para realização de vistorias técnicas agendadas. A vistoria, **que é facultativa**, visa permitir o conhecimento dos equipamentos ou da rede, das instalações, da natureza e das condições de execução dos serviços.

4.2– Para realização da referida vistoria, o representante legal da licitante, devidamente identificado, **deverá** assinar o Termo de Confidencialidade, conforme modelo disponível no Anexo n. 12.

4.2.1- O Termo de Confidencialidade deverá ser assinado em duas vias, uma das quais ficará em posse do Centro de Informática da Câmara dos Deputados e a outra será entregue à licitante.

4.3- A vistoria técnica será agendada por meio do telefone (61) 3216-3793.

4.4- Não serão aceitas alegações posteriores advindas de desconhecimento das condições dos equipamentos, da rede, das instalações e do ambiente da Câmara dos Deputados, referentes aos serviços objeto desta licitação.

5- DA REPACTUAÇÃO DO PREÇO

O preço global mensal contratado referente aos serviços de garantia de funcionamento e atualização poderá ser repactuado, desde que observado interregno mínimo de 1 (um) ano, a contar da data da proposta, ou da data do orçamento a que a proposta se referir, ou da data da última repactuação, cabendo à Contratada, na oportunidade de sua solicitação, justificar e comprovar a variação dos componentes dos custos do Contrato, apresentando, inclusive, Memória de Cálculo e Planilhas apropriadas para análise e posterior aprovação da Contratante.

6-DO ÓRGÃO FISCALIZADOR

Considera-se órgão fiscalizador o Centro de Informática - CENIN da Câmara dos Deputados, situado no 11º andar do Edifício Anexo I, que designará servidor responsável pelos atos de acompanhamento, controle e fiscalização do contrato.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 2

PREGÃO ELETRÔNICO N. 52/10

ESPECIFICAÇÕES TÉCNICAS

1. ..Zero.1- ESPECIFICAÇÕES TÉCNICAS

1.1. Gerenciamento via console(s) central(is) de um mesmo fabricante.

1.1.1. Define-se solução de mesmo fabricante a que foi implementada a partir de componentes próprios ou incorporados por meio de aquisições ou fusões.

1.1.2. Serão admitidos, no máximo, 3 (três) consoles centrais de um mesmo fabricante para gerenciar todos as funcionalidades da solução *Endpoint*.

1.1.3. Deverá prover alta disponibilidade por meio de uma das formas abaixo:

1.1.3.1. Balanceamento de carga do número de agentes instalados nos computadores entre duas ou mais consoles centrais de gerenciamento.

1.1.3.2. Duas ou mais consoles centrais de gerenciamento funcionando no modo de *cluster* ativo-ativo ou ativo-passivo.

1.2. Console(s) de gerenciamento:

1.2.1. Armazenamento centralizado de registros (logs);

1.2.2. Download automático de atualizações ou por comando dos administradores a partir do site do fabricante da solução.

1.2.3. Prover mecanismo para desinstalação de atualizações de forma centralizada.

1.2.4. Distribuição automática de políticas e atualizações via rede ou por comando pelos administradores.

1.2.5. Aplicação de políticas segundo os seguintes critérios:

1.2.5.1. Todos os agentes;

1.2.5.2. Grupos de agentes ou estações;

1.2.5.3. Agente ou estação específica.

1.2.6. Personalização das notificações que serão exibidas aos usuários para o idioma português (Brasil).

1.2.7. Gerência de todas as funcionalidades da solução por meio de interface gráfica.

1.2.8. Interface gráfica para a geração de relatórios sobre o funcionamento da solução e sobre os dados coletados por meio do(s) agente(s).

1.2.9. Definição de grupos de usuários e equipamentos a serem utilizados nas políticas.

1.2.10. Integração com o Microsoft Active Directory 2003 e superior, incluindo minimamente, a capacidade de importação e sincronização de usuário, grupos de usuários, máquinas e grupos de máquinas presentes no Active Directory.

1.2.11. Granularidade para atribuir níveis de acesso de leitura ou controle total às funcionalidades da solução de Endpoint. aos usuários do(s) console(s).

1.2.12. Sistema de auditoria para registrar todas as ações executadas pelos usuários do(s) console(s) de gerenciamento.

1.2.13. Controle dos intervalos de comunicação entre o(s) console(s) de gerenciamento e o(s) agente(s) local(is).

1.2.14. Gerar alertas e relatórios contendo a lista de máquinas desatualizadas.

1.2.15. Definir o prazo mínimo para que uma máquina seja considerada desatualizada (por exemplo, uma máquina será considerada desatualizada se o *antimalware* não foi atualizado nos últimos 5 dias).

1.3. Agente(s) local(is):

1.3.1. Compatibilidade com Microsoft Windows Vista/XP/2000 Professional em português e Microsoft Windows 2000 Server, Windows Server 2003 e superiores em inglês.

1.3.2. Instalação e desinstalação de forma automática por um dos seguintes métodos:

1.3.2.1. Console(s) de gerenciamento;

1.3.2.2. via *prompt* de comando (*shell*);

1.3.2.3. criação de pacote de instalação no formato .msi ou .exe a ser usado por sistema especializado na distribuição de software.

1.3.3. Funcionamente off-line, operando com a última política recebida, enquanto não for restabelecida a comunicação com o(s) console(s) de gerenciamento.

1.3.4. Uso de políticas diferentes quando a estação estiver conectada à rede interna (com acesso ao domínio Active Directory) e quanto estiver conectada a outras redes.

1.4. Relatórios e registros (*logs*).

1.4.1. Relatórios:

1.4.1.1. Lista de máquinas desatualizadas;

1.4.1.2. detalhamento dos casos de *malware* detectados;

1.4.1.3. máquinas e usuários com mais arquivos infectados;

1.4.2. Manutenção de registros (*logs*) de todas as ações executadas pelo(s) agente(s).

1.4.2.1. Os registros deverão incluir todas as ações executadas pelo(s) agente(s) local(is).

1.4.2.2. Os registros poderão ser armazenados temporariamente nas estações, mas deverão ser transferidos para o(s) console(s) de gerenciamento automaticamente em intervalos regulares.

1.4.2.3. Definição de um tamanho máximo a ser ocupado pelos arquivos de *log* nas estações.

1.4.2.3.1. Implementar rotação de *logs*.

1.4.2.4. Exportação dos *logs* no formato texto simples (*ANSI* ou *Unicode* (UTF8) ou *Unicode* (UTF16)), CSV (separado por vírgulas) ou HTML / XML.

1.4.2.5. Suporte ao banco de dados Microsoft SQL Server 2000 e superiores.

FUNCIONALIDADES DA SOLUÇÃO ENDPOINT

1.5. AntiMalware (*spyware*, *adware*, vírus, cavalos de tróia, *rootkits* e outros códigos maliciosos)

1.5.1. Prover atualizações, no máximo, diárias das definições de *malware* utilizadas. As atualizações deverão ser obtidas pelo(s) console(s) de gerenciamento e distribuídas ao(s) agente(s) local(is) automaticamente.

1.5.2. Implementar as seguintes formas de varredura contra *malwares* em memória RAM, arquivos, *Registry* e *cookies*:

1.5.2.1. Varredura agendada com definição de horários para a verificação das máquinas;

1.5.2.2. habilitação e desabilitação dos agendamentos;

1.5.2.3. agendamentos diários, semanais, ao iniciar o sistema operacional e no logon do usuário;

1.5.2.4. varredura tempestiva em uma estação ou grupo de estações, com comando por meio do(s) console(s) de gerenciamento.

1.5.3. Varredura em tempo real (on-access scanner).

1.5.4. Varredura heurística para:

1.5.4.1. Detectar arquivos executáveis que tenham código malicioso ou programas potencialmente indesejados.

1.5.4.2. Procurar vírus desconhecidos.

1.5.5. Configuração de um período de tempo máximo para as varreduras e cancelamento automático em caso de expiração.

1.5.6. Execução de varreduras por linha de comando ou a partir de arquivos de batch ou scripts.

1.5.7. Opções para quando uma ameaça for encontrada:

1.5.7.1. Ação principal: “Limpar automaticamente”, “Negar acesso ao arquivo” ou “Excluir automaticamente” ou ações similares.

1.5.7.2. Ação secundária: “Negar acesso ao arquivo”, “Excluir automaticamente”, “Mover arquivo para área de quarentena” ou “Continuar varredura” ou ações similares.

1.5.8. Formas de classificação e detecção de programas indesejados:

1.5.8.1. Vírus, *spyware*, *adware, worms*, discadores, capturadores de digitação (*Keyloggers*), ferramentas de administração remota.

1.5.8.2. Detecção baseada em nomes de arquivos definidos pelo administrador por meio do(s) console(s) de gerenciamento.

1.5.9. Excluir da varredura arquivos, diretórios, chaves de *Registry* ou *cookies* específicos definidos pelo administrador.

1.5.10. Opções de exame para todos os tipos de varredura:

1.5.10.1. Todos os arquivos;

1.5.10.2. Extensões pré-definidas contidas em lista inicial de extensões perigosas e permitir a inclusão de outras extensões.

1.5.11. Cadastrar extensões que não devem ser verificadas.

1.5.12. Verificar arquivos compactados nos formatos mais utilizados em nível configurado pelo administrador da solução de Endpoint e codificados MIME.

1.5.12.1. Configurar tempo máximo de varredura para esses arquivos.

1.5.12.2. Varredura de arquivos aninhados (*nested files*), ou seja, verificar arquivos compactados que estejam dentro de outros arquivos compactados.

1.5.12.3. Configuração do nível máximo de aninhamento de compactadores e ação a ser executada.

1.5.13. Verificar arquivos de macro e verificar macros em arquivos de programas de escritório (Microsoft Office, BrOffice e similares).

1.5.14. Definição do uso máximo de CPU pelo(s) agente(s) local(is) para cada varredura agendada.

1.5.15. Manutenção de registros (logs) de todas as ações executadas.

1.5.16. Impedir a execução de scripts e programas nas pastas de armazenamento temporário (por exemplo, c:\temp, pastas temp privativas dos usuários, “Temporary Internet files”).

1.5.17. Classificação “Advanced” nos testes do AV-comparatives (www.av-comparatives.org) ou ter sido aprovado em um dos dois últimos testes VB100 da Virus Bulletin (www.virusbtn.com).

1.5.18. Recurso de “roll back” automático ou manual, via console de gerenciamento, em caso de detecções “falsos positivas” ocorridos depois de instalação de arquivo de assinatura de código malicioso ou equivalente.

1.6. *Firewall* pessoal

1.6.1. Ativação ou desativação do firewall por máquinas ou grupos de máquinas.

1.6.2. Importar as configurações de firewall de uma estação de trabalho e aplicá-la a outra estação ou a um grupo de estações.

1.6.3. Criação, alteração e exclusão de lista autorizada (white list) e não autorizada (black list) de execução de programas. As aplicações da lista autorizada sempre terão permissão de execução nas estações. As aplicações da lista não autorizada nunca terão permissão de execução nas estações.

1.6.4. Criação, alteração e exclusão de listas autorizada (white list) e não autorizada (black list) de endereços IP. Os endereços da lista autorizada sempre terão permissão de acesso via rede às estações. Os endereços da lista não autorizada nunca terão permissão de acesso via rede às estações.

1.6.5. Criação e aplicação remota de políticas distintas de firewall a grupos diferentes de máquinas.

1.6.6. Iimplementar política que permita que apenas uma interface de rede esteja ativa em cada estação.

1.6.7. Recursos para impedir o desligamento das políticas de firewall por atacantes ou malware.

1.6.8. Filtragem por tipo de tráfego, aplicação que envia ou recebe dados e assinaturas de ataques conhecidos.

1.6.9. Por meio da interface gráfica do(s) console(s) de gerenciamento, o firewall deverá possuir os seguintes itens de configuração:

1.6.9.1. Habilitar ou desabilitar detecção de intrusão;

1.6.9.2. Exibir ou não mensagem de notificação de ataque;

1.6.9.3. Quando estiver sob ataque:

1.6.9.3.1. Habilitar ou não exibição de mensagem;

1.6.9.3.2. Permitir envio de email aos administradores.

1.6.10. Assinaturas de ataque de Port scan (UDP e TCP), Syn flood e PPTP buffer overflow.

1.6.11. Regras baseadas em tipo de conexão, protocolos IP e não IP, direção do tráfego de rede, aplicação geradora do tráfego, serviço ou porta usada pelo computador, endereço IP usado no pacote.

1.6.12. Recurso de duplicação de regras existentes.

1.6.13. Níveis de proteção baixo, alto e personalizado

1.7. Host-Based Intrusion Prevention System – HIPS

1.7.1. Regras baseadas em:

1.7.1.1. Protocolos IP e não IP.

1.7.1.2. Direção do tráfego (entrada, saída ou ambas).

1.7.1.3. Tipo de conexão (rede ou sem fio).

1.7.1.4. Aplicações que geraram o tráfego.

1.7.1.5. Serviço ou porta usados pelo computador local.

1.7.1.6. Serviço ou porta usados pelo computador remoto.

1.7.1.7. Endereços IP de origem ou destino.

1.7.1.8. Conteúdo dos pacotes.

1.7.2. Modelos de políticas personalizáveis para aplicações e configurações mais usuais.

1.7.3. Habilitar ou desabilitar as políticas em estações ou grupos de estações.

1.7.4. Definição de políticas para permitir ou bloquear a execução de determinadas aplicações.

1.7.5. Ações de registrar (log) ou impedir execução.

1.7.6. Configuração de notificações de alerta por email.

1.7.7. Tipos de bloqueio de execução:

1.7.7.1. Execução de aplicação (criação de processo) e

1.7.7.2. Anexação (*hook*) de código a um processo em execução.

1.7.8. Criação de exceções às políticas (classificar aplicações como confiáveis).

1.7.9. Assinaturas para proteção contra ataques de rede e atualização periódica.

1.8. *Network Access Control* – NAC

1.8.1. Compatibilidade com 802.1x (via software ou hardware - appliances) ou Microsoft Network Access Protection (NAP)

1.8.2. Bloquear ou colocar sob regime de quarentena os dispositivos que tentarem se conectar à rede da Câmara dos Deputados e não atenderem aos requisitos de segurança, impedindo o acesso à rede local e recursos compartilhados.

1.8.3. Conformidade do dispositivo tentando conectar à rede da Câmara, tais como: versão da base de dados de malware, firewall configurado conforme as políticas corporativas e ativo, service packs e patches de segurança do sistema operacional atualizados.

1.8.4. Identificar os sistemas não gerenciados (que não possuem o(s) agente(s) local(is) instalado(s)) e aplicar política específicas para esses sistemas.

1.8.5. Definir tipos ou grupos de sistemas. Deverá permitir a definição de políticas de conformidade específicas para cada grupo ou tipo de sistema.

1.8.6. Definição de níveis diferentes de acesso à rede, dependendo da violação da política de acesso que foi identificada.

1.8.7. Configurações de máquinas ou grupos de máquinas isentos das políticas de NAC.

1.8.8. Remediação automaticamente. A remediação deverá incluir todas as ações necessárias para deixar o sistema conforme a política aplicável.

1.8.8.1. Funcionalidade de exibição de mensagens de não conformidade aos usuários, listando os problemas encontrados e procedimentos para restaurar o estado de conformidade da estação.

1.8.9. Definição de quando avaliar a conformidade de sistemas por meio de varreduras.

1.8.9.1. No início do sistema;

1.8.9.2. Quando um sistema é reconectado à rede ou se houver mudança no estado do adaptador de rede;

1.8.9.3. Quando o console do servidor NAC solicitar.

1.8.10. Agendamento de varredura de clientes gerenciados pelo(s) console(s) de gerenciamento. A solução deve prover mecanismo para habilitar ou desabilitar o agendamento para grupos de máquinas definidas no(s) console(s) de gerenciamento.

1.8.11. Mínimo, 2 (dois) modos de funcionamento (*enforcement*):

1.8.11.1. Aplicar (*enforce*) a política, restringindo o acesso à rede.

1.8.11.2. Apenas monitorar e registrar os casos de não conformidade.

1.8.12. Exportação e importação de políticas de conformidade de Endpoint.

1.8.13. Relatórios

1.8.13.1. Via console de gerenciamento, monitoração do acesso à rede (quantidade de máquinas em conformidade (*compliant*) com as políticas e em não conformidade.

1.9. Prevenção ao vazamento de dados corporativos (*Data Loss Prevention*)

1.9.1. Funcionalidade de *Data Loss Prevention* ou prover integração com as principais soluções de DLP existentes no mercado.

1.10. Criptografia de discos rígidos

1.10.1. Método que permita ao administrador recuperar acesso a dados criptografados de forma controlada e somente quando for necessário.

1.10.2. Método de criptografia persistente, independentemente do sistema de arquivo destino (FAT, FAT32, NTFS).

1.10.3. Suporte à criptografia de todo o disco rígido (ou de partições completas) com autenticação antes ou durante o pré-carregamento do sistema operacional.

1.10.4. Implementar o algoritmo AES com chaves de 256 bits conforme o padrão FIPS 197.

1.10.5. Suportar as recomendações do NIST SP800-111 (Guide to Storage Encryption Technologies for End User Devices).

1.10.6. Padrão IEEE 1619.

1.10.7. Uso de *tokens* ou *smart cards* com certificados digitais como mecanismo de autenticação.

1.11. Controle de dispositivos

1.11.1. Controle de interfaces PCMCIA, USB 1.0, 1.1 e 2.0, Firewire, ATAPI, Serial (COM), Paralela, IrDA, SCSI, Bluetooth.

1.11.2. Controle de d*rives* de disco, *pen drives*, dispositivos de imagem, adaptadores de vídeos, teclados, leitores de *smart card*, *drives de CD-ROM/DVD*, *mouse* e outros dispositivos apontadores, controladores de som, vídeo e jogos, *drives* de disquete, *drives* de fita e dispositivos de interface humana (HID), dispositivos *ACPI* específicos, PDAs (*Palm*, *Windows* e similares), controladores de cartão de memória.

1.11.3. Modo de aprendizado para dispositivos que são específicos de um fabricante. O aprendizado deverá permitir que a solução passe reconhecer o dispositivo e possa gerenciá-lo.

1.11.4. Granularidade para que alguns dispositivos específicos sejam permitidos, mesmo que a política geral os bloqueie. A solução deverá possibilitar aos administradores permitir o uso dos dispositivos com base em número de série, modelo e/ou fabricante.

1.11.5. Aplicação de políticas específicas para grupos de máquinas e usuários definidos no Active Directory.

1.11.6. Executar atualização de políticas quando usuário efetuar login.

1.11.7. Manutenção das políticas mesmo que esteja desconectada da rede e sem acesso ao(s) console(s) de gerenciamento.

1.11.8. Permissões de acesso:

1.11.8.1. Leitura; Leitura e escrita; Bloqueio.

1.12. Antimalware para *Exchange Server* 2003 e superior

1.12.1. Integrar gerenciamento de antimalware ao(s) console(s) de gerenciamento.

1.12.2. Integração com Active Directory da Microsoft.

1.12.3. Compatibilidade com as APIs de varredura de código malicioso da Microsoft listadas em http://support.microsoft.com/kb/823166.

1.12.4. Atualização automática dos arquivos de assinatura de códigos maliciosos.

1.12.5. Filtragem de mensagens eletrônicas de entrada e saída.

1.12.6. Identificação de tipo de arquivo e capacidade de filtragem de busca e remoção de anexos e anexos aninhados em arquivos compactados.

1.12.7. Recurso de gerenciamento de surtos de código malicioso baseado em regras.

1.12.8. Aplicação políticas de grupo a usuários como exceção à política global.

1.12.9. Alerta de descarte de mensagens infectadas por código malicioso.

1.12.10. Registros (*logs*) consolidados no(s) console(s) de gerenciamento.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 3

PREGÃO ELETRÔNICO N. 52/10

CAPACITAÇÃO OPERACIONAL

1- DAS DISPOSIÇÕES PRELIMINARES

1.1. A capacitação operacional deverá ser concluída dentro do prazo para execução da Fase 1 do Cronograma de Encadeamento das Fases disposto no Anexo n. 4 e ser executada conforme as exigências deste anexo.

1.2. A conclusão da capacitação operacional é pré-requisito à concessão do aceite provisório da Fase 1.

1.3. As aulas deverão ser ministradas fora das dependências da Câmara dos Deputados, obrigatoriamente em Brasília (DF), em local disponibilizado pela contratada e apropriado para a consecução de treinamentos, com adequado mobiliário e conforto térmico, acústico e luminoso, em ambiente seguro e que possua todos os insumos, recursos e equipamentos para o perfeito desempenho das atividades de treinamento.

1.4. A capacitação operacional deverá habilitar 5 (cinco) servidores da Câmara dos Deputados na utilização da solução *Endpoint* e deverá ter duração mínima de 20 (vinte) horas.

1.5. O curso de capacitação deverá ter duração diária máxima de 4 (quatro) horas, salvo se acordado de forma diferente entre as partes e deverá ser realizado em dias úteis e consecutivos. O turno de realização da capacitação operacional será determinado pelo órgão fiscalizador da Contratante.

1.6. A Contratada configurará ambiente físico apropriado equivalente à rede local corporativa da Câmara dos Deputados, com os mesmos *softwares* e versões fornecidos e fornecerá material didático impresso que aborde todo o conteúdo programático, em até 3 (três) dias úteis antes do início da capacitação operacional.

1.6.1. É vedada a utilização dos equipamentos instalados na Câmara dos Deputados para a capacitação operacional.

1.6.2. Todo e qualquer material didático previsto pelo fabricante do produto ou necessário ao treinamento deverá ser fornecido pela contratada.

1.7. A contratada fornecerá aos participantes da capacitação operacional os respectivos certificados oficiais de conclusão.

1.8. A capacitação operacional deverá ser focada nas funcionalidades da solução que atendam às necessidades da Câmara dos Deputados.

1.9. O curso oferecido não deverá sofrer redução de sua duração prevista pelo fornecedor da solução *Endpoint.*

2- DO INSTRUTOR

2.1. A Câmara dos Deputados reserva-se o direito de, por intermédio do órgão fiscalizador e até o segundo dia útil após o início da capacitação operacional, solicitar a substituição de instrutor que venha a ser considerado didaticamente inadequado pela maioria simples dos treinandos.

2.2. Caso solicitada, a substituição deverá ser promovida em, no máximo, 5 (cinco) dias, contados da solicitação do órgão fiscalizador à contratada.

2.2.1. Nesse caso, o conteúdo programático deverá ser reiniciado.

3- DO PROGRAMA DE CAPACITAÇÃO OPERACIONAL

3.1. Descrição técnica do funcionamento da solução.

3.2. Procedimentos iniciais (Identificação dos requisitos de software, instalação da solução, políticas de segurança corporativa, preparação de clientes e computadores servidores).

3.3. Distribuição do(s) cliente(s) Preparação da instalação, métodos disponíveis de instalação, instalação do(s) cliente(s), varredura do(s) cliente(s), gerenciamento do ambiente do usuário final.

3.4. Instalação ou configuração de componentes adicionais (computador servidor central para recepção e distribuição das atualizações aos clientes).

3.5. Configurando políticas de antivírus e anti-spyware (ajustes gerais, varreduras de autoproteção e definidas pelo administrador, quarentena de arquivos).

3.6. Configurações adicionais (varredura pró-ativa, exceções, outras proteções).

3.7. Gerenciamento (visualização e gerenciamento de logs, notificações e relatórios, administração e segurança dos computadores servidores de gerência, comunicação com outros computadores servidores, gerenciamento de administradores e da bases de dados).

3.8. Projeto de implementação de segurança de *Endpoint*.

3.9. Proteção de ameaças de rede e controle de dispositivos (*firewall*, regras de *firewall*, filtragem de tráfego, configuração HIPS, gerenciamento de assinaturas personalizadas, NIPS, criação e personalização de políticas de controle de aplicações e dispositivos, gerenciamento de grupos, componentes de políticas e aprendizado de aplicação).

3.10. Configurações de performance.

3.11. Resolução de problemas da solução *Endpoint*.

4- DA AVALIAÇÃO DA CAPACITAÇÃO OPERACIONAL

4.1. Os participantes preencherão no último dia de aula questionários de avaliação da capacitação operacional, conforme modelo constante do Título 5 deste anexo.

4.2. O questionário abordará:

4.2.1. abrangência dos tópicos abordados;

4.2.2. aplicabilidade dos tópicos abordados;

4.2.3. instalações físicas;

4.2.4. material didático;

4.2.5. recursos disponíveis.

Quanto ao instrutor:

4.2.6. capacidade de harmonizar teoria e prática;

4.2.7. capacidade de utilizar técnicas e recursos que facilitem a aprendizagem;

4.2.8. clareza na exposição de idéias;

4.2.9. pontualidade;

4.2.10. segurança e domínio do conteúdo.

4.3. Cada um dos aspectos descritos no item 4.2 anterior será avaliado mediante os seguintes critérios a serem indicados pelos participantes: ótimo, bom, regular, ruim, péssimo.

4.4. O órgão fiscalizador comunicará formalmente à Contratada o resultado da avaliação realizada, no prazo máximo de dez dias, contados do encerramento da capacitação operacional.

4.5. Caso quatro ou mais dos subitens 4.2.1 a 4.2.10 deste anexo tenham avaliação ruim ou péssima por mais de 50% (cinqüenta por cento) dos treinandos, a Contratada deverá reeditar a capacitação operacional, sem ônus adicional para a Câmara dos Deputados.

5- DO MODELO DO QUESTIONÁRIO DE AVALIAÇÃO

Avaliação da Capacitação Operacional

Nome do aluno: (opcional)	
Período:	

Favor assinalar com um "X" no campo que expresse sua avaliação a respeito do aspecto:

Aspecto	péssimo	ruim	regular	bom	ótimo
Abrangência dos tópicos abordados					
Aplicabilidade dos tópicos abordados					
Instalações físicas					
Material didático					
Recursos disponíveis					
Instrutor					
Capacidade de harmonizar teoria e prática					
Capacidade de utilizar técnicas e recursos que facilitem a aprendizagem					
Clareza na exposição de idéias					
Pontualidade					
Segurança e domínio do conteúdo					
Observações do participante:					

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 4

PREGÃO ELETRÔNICO N. 52/10

INSTALAÇÃO DA SOLUÇÃO E CRONOGRAMA DE ENCADEAMENTO DAS FASES

1- DA INSTALAÇÃO DA SOLUÇÃO

1.1 A instalação da solução obedecerá ao cronograma de Encadeamento das Fases, conforme descrito neste anexo. Os prazos máximos para conclusão de cada fase serão rigorosamente obedecidos, podendo implicar, o seu descumprimento, aplicação de multa, conforme Anexo n. 8 deste Edital.

1.2. Ao término das Fases 1 e 2, se atendidas as exigências deste Edital, será concedido o Aceite Provisório das respectivas fases, ficando o Aceite Provisório da Solução condicionado à conclusão da Fase 3, quando deverá ter sido realizada toda a implementação da solução E*ndpoint* e esta deverá estar em pleno funcionamento, com todas as funcionalidades requeridas pelo órgão fiscalizador.

1.2.1. A Fase 4 está prevista para ser executada a partir de junho de 2010, a partir da data do envio da Ordem de Serviço (subitem 2.4.2 deste anexo) e, após a sua conclusão em conformidade com as exigências deste Edital, será emitido o Aceite Definitivo da Solução.

1.3. A solução *Endpoint* será instalada nas dependências da Câmara dos Deputados, em Brasília-DF.

1.4. A instalação será realizada pela contratada utilizando-se da infraestrutura que estará disponível até o início dos procedimentos, sendo os serviços realizados sob a supervisão do órgão fiscalizador.

1.5. A instalação dos agentes locais incluirá a remoção do software antimalware atualmente instalado nas estações da Câmara do Deputados se for de outro fabricante.

1.6. Durante a Fase 2, a Câmara dos Deputados poderá solicitar a implementação de novas funcionalidades disponíveis na solução.

1.7. A entrega da documentação com insuficiência e/ou inconsistências de informações, poderá implicar, para todos os efeitos e até a sua complementação e/ou correção, aplicação de multa, conforme Anexo n. 8 deste Edital.

2- DA DESCRIÇÃO DAS FASES

2.1. FASE 1

2.1.1. Entrega dos componentes das funcionalidades previstas nos subitens 1.1 a 1.5 do objeto da licitação contido no Anexo n. 1.

2.1.2. Da capacitação operacional

2.1.2.1. A capacitação operacional terá que ser concluída no prazo previsto para o término da Fase 1.

2.1.2.2. A capacitação operacional habilitará servidores da Câmara ao uso pleno de todos os recursos da solução *Endpoint* fornecida, nos termos descritos no Anexo n. 3.

2.2. FASE 2 – Instalação, Configuração.e Ativação da Solução – Subitem 1.1 a 1.5 do objeto da licitação contido no Anexo n. 1

A solução *Endpoint* será instalada de acordo com os termos e condições abaixo:

2.2.1. O prazo para execução desta fase será contado a partir do aceite provisório da Fase 1.

2.2.2. A instalação e configuração da solução *Endpoint* deverá ser feita por técnico certificado pelo fabricante.

2.2.3. Instalação e configuração de todos os componentes da solução, conforme estabelecido pelo órgão fiscalizador, tornando-a disponível para entrar em operação.

2.2.4. Instalação de todas as correções de software *patches* disponíveis e pertinentes.

2.2.5. Integração ao ambiente da rede de dados da Câmara dos Deputados, efetuando todas as configurações necessárias ao seu pleno funcionamento, especialmente com a solução de gerenciamento de estações da Corel.

2.2.6. Configurar procedimentos de *backup* e recuperação de todos os componentes da solução *Endpoint*. Os procedimentos de restauração serão devidamente atestados pelo órgão fiscalizador.

2.2.7. Alteração de todas as configurações *default* do equipamento (portas lógicas de acesso ao equipamento, mensagens geradas pelo software *Endpoint*, etc.) de forma a minimizar o risco de identificação da solução *Endpoint* por atacantes e exploração de vulnerabilidades conhecidas.

2.2.8. Concluídas a instalação e configuração, a contratada apresentará documentação completa, em meio eletrônico, até a data de conclusão da presente fase, abrangendo a topologia e a configuração dos serviços executados, sendo essa apresentação indispensável à concessão do aceite provisório. A documentação apresentará, no mínimo, as seguintes informações:

2.2.8.1. Todo o processo de instalação e configuração da solução *Endpoint*.

2.2.8.2. Todas as permissões do sistema de arquivos modificadas durante os processos de instalação e configuração, se aplicável.

2.2.8.3. Todas as configurações dos componentes, incluindo configurações de *hardware* que se façam necessárias.

2.2.8.4. Processos não documentados pelo fabricante que dizem respeito à instalação e configuração da solução.

2.2.8.5. Erratas lançadas após a documentação impressa ou com data posterior à documentação eletrônica.

2.2.8.6. Todas as informações sobre correções *patches* aplicadas na solução *Endpoint*, incluindo documentação fornecida pelo fabricante.

2.2.8.7. Os subsídios citados acima incluem recomendações de ativação.

2.2.9. A forma de ativação da solução será definida pelo órgão fiscalizador da Contratante, conforme orientação da Contratada, no que diz respeito à configuração de todas as funcionalidades, instalação única ou por funcionalidade da solução e aplicação gradual em toda rede.

2.3. FASE 3 - Distribuição das funcionalidades configuradas nos equipamentos em rede – Subitem 1.1 a 1.5 do objeto da licitação contido no Anexo n. 1

2.3.1. Serão distribuídas e ativadas nesta fase todas as funcionalidades da solução *Endpoint* nos equipamentos de rede, exceto aquelas referentes ao subitem 1.9 do item único do objeto da licitação contido no Anexo n. 1.

2.3.2. A contratada deverá propor cronograma de implantação da solução em toda a rede local corporativa e prestar o devido suporte.

2.3.3. O cronograma deverá ser baseado em melhores práticas de ativação das funcionalidades de *Endpoint,* observado o disposto no subitem 2.2.9 deste anexo.

2.3.4. Caso o cronograma proposto pela contratada não possa ser executado por impedimentos da Câmara, esse será reajustado em comum acordo.

2.4. FASE 4 – Licenciamento, Instalação e Distribuição dos componentes da funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS) referentes ao subitem 1.9 do item único do objeto da licitação contido no Anexo n. 1.

2.4.1. A partir de junho de 2010 o órgão fiscalizador enviará à contratada, por meio eletrônico, uma Ordem de Serviço referente ao licenciamento, à instalação e distribuição dos componentes da funcionalidade (subitem 1.9 do objeto da licitação contido no Anexo n. 1), contando-se, a partir daí, o prazo para conclusão da Fase 4.

2.4.2. A contratada deverá, no prazo máximo de um dia útil, contado da data do envio da Ordem de Serviço, confirmar o seu recebimento, por meio eletrônico.

3- DO CRONOGRAMA DE ENCADEAMENTO DAS FASES

3.1. No cronograma apresentado abaixo, os dias úteis definidos destinam-se a ações de responsabilidade exclusiva da contratada e não incluem os dias corridos despendidos pelo órgão fiscalizador nas análises e aferições necessárias à concessão dos aceites provisórios e/ou definitivo das fases descritas.

Fases	**Período 1 (Prazo de execução)**	**Período 2 (Prazo de execução)**	**Período 3 (Prazo de execução)**	**Percentual (*)**
Fase 1 - Entrega dos Componentes (subitens 1.1 a 1.5 do item único do objeto da licitação contido no Anexo n. 1) e Capacitação Operacional. (Emissão de Aceite Provisório da Fase 1.)	Quinze dias úteis, contados da data de assinatura do contrato	-----	-----	-----
Fase 2 – Instalação, Configuração e ativação da solução (subitens 1.1 a 1.5 do item único do objeto da licitação contido no Anexo n. 1) (Emissão de Aceite Provisório da Fase 2.)	------	Dez dias úteis, contados da data do aceite provisório da Fase 1	-----	**40%**
Fase 3 – Distribuição das funcionalidades configuradas nos equipamentos em rede (subitens 1.1 a 1.5 do item único do objeto da licitação contido no Anexo n. 1). (Emissão do Aceite Provisório da Solução.)	------	Sessenta e cinco dias úteis, contados da data do aceite provisório da Fase 2	-----	**30%**
Duração (Fases 1 a 3):Noventa dias úteis				
Fase 4 – Licenciamento, Instalação e Distribuição (subitens 1.9 e 1.10 do item único do objeto da licitação contido no Anexo n. 1) (Emissão do Aceite Definitivo da Solução.)	------	------	Quinze dias úteis, contados da data do envio da Ordem de Serviço **(A partir de Junho/2010)**	**30%**

(*) **Percentual sobre o** somatório dos valores referentes aos subitens 1.1 a 1.7, 1.9 e 1.10 do item único objeto da licitação contido no Anexo n. 1, disposto no Anexo n. 1 deste Edital (excluído os valores referentes aos pagamentos mensais dos serviços de garantia de funcionamento (suporte técnico) e atualização.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 5

PREGÃO ELETRÔNICO N. 52/10

SERVIÇOS DE SUPORTE TÉCNICO E ATUALIZAÇÃO

1-DAS CONDIÇÕES GERAIS PARA EXECUÇÃO DO SUPORTE TÉCNICO

1.1. O suporte técnico será prestado como uma série de procedimentos efetuados pela contratada destinados a auxiliar a equipe técnica da Câmara dos Deputados na prevenção e resolução de problemas na solução *Endpoint* fornecida, bem como na otimização ou ajustes nas configurações desta.

1.1.1. Todos os chamados deverão ser atendidos pelo técnico indicado na Reunião Preparatória conforme item 11.7 do Edital.

1.1.2. Caso haja substituição do referido técnico durante o período de vigência do contrato, deverão ser cumpridas todas as exigências dispostas no subitem 11.7.1 do Edital, relativas à documentação e aprovação do técnico.

1.2. O órgão fiscalizador, com periodicidade mensal, solicitará à contratada a execução de procedimentos necessários à análise das configurações e dos arquivos de registros (*logs*) da solução Endpoint com o objetivo de prevenir falhas e otimizar o desempenho.

1.3. A contratada, em até cinco dias após a data de assinatura do contrato, informará por meio do correio eletrônico seseg.cenin@camara.gov.br os meios para abertura de chamados técnicos (email, fax, telefone fixo, telefone celular, bip, sítio Internet, etc).

1.4. No registro das solicitações de suporte técnico serão fornecidas as seguintes informações:

1.4.1. Criticidade do chamado.

1.4.2. Descrição do serviço a ser executado ou da anormalidade observada.

1.4.3. Nome do responsável pela solicitação do serviço.

1.5. O suporte técnico deverá estar disponível 24 (vinte e quatro) horas por dia, de Segunda a Sábado.

1.6. Todos os prazos mencionados neste anexo serão contados a partir da data e da hora do registro da solicitação técnica.

1.7. Para efeito de aplicação de multas previstas no Anexo n. 8 deste Edital, os dias em atraso serão contados a partir do final dos prazos estabelecidos neste anexo.

2-DOS PRAZOS E DAS CONDIÇÕES DE ATENDIMENTO

2.1. Os chamados serão classificados nos seguintes tipos de severidade:

2.1.1. Crítica: Solução totalmente parada ou causando grande impacto no ambiente de produção. Deverá ser recolocada em funcionamento normal em até um dia.

2.1.2. Alta: Solução com funcionalidades importantes parcialmente paradas. Deverá ser recolocada em funcionamento normal em até dois dias.

2.1.3. Média: Solução com erros ou problemas que causam impacto moderado no ambiente de produção. Deverá ser recolocada em funcionamento normal em até cinco dias.

2.1.4. Baixa: Solução com erros ou problemas que causam pouco impacto no ambiente de produção. Deverá ser recolocada em funcionamento normal em até dez dias.

2.1.5. Preventiva/evolutiva: Consultas técnicas, atualizações, implementação de novas funcionalidades e resolução de dúvidas em geral. Deverá ser resolvida em até quinze dias.

3-DOS RELATÓRIOS TÉCNICOS

3.1. As solicitações de suporte técnico feitas pelo órgão fiscalizador serão registradas pela contratada para acompanhamento e controle da execução dos serviços.

3.2. A contratada apresentará ao órgão fiscalizador relatório de atendimento contendo data e hora da solicitação, início e término do atendimento, identificação do defeito, diagnóstico do problema, soluções provisórias, soluções definitivas, hipóteses sob investigação, dados que comprovem o diagnóstico, assim como dados e circunstâncias julgados necessários ao esclarecimento dos fatos, nome do técnico responsável pela execução do serviço, as providências adotadas e outras informações pertinentes.

3.3. Após o atendimento da solicitação, o relatório será assinado por funcionário do órgão fiscalizador confirmando a execução dos serviços.

3.4. A omissão da entrega do relatório técnico no prazo máximo de cinco dias úteis poderá implicar aplicação de multa, conforme Anexo n. 8 deste Edital.

4-OUTROS ASPECTOS RELACIONADOS À EXECUÇÃO DO SUPORTE TÉCNICO

4.1. A Câmara dos Deputados poderá efetuar configurações na solução e implementar novas funcionalidades sem prejuízo das condições de garantia de funcionamento previstas neste Edital.

4.2. O prazo máximo para comunicação de disponibilidade de novas versões dos softwares, caso a solução não informe automaticamente, é de dez dias úteis contados da data de lançamento comercial.

4.3. A Câmara dos Deputados poderá submeter à contratada arquivo(s) suspeito(s) de conterem código malicioso. A contratada, comprovando a suspeita, terá até 24 (vinte e quatro) horas, contadas da submissão do(s) arquivo(s), para disponibilizar vacinas para detecção e remoção do código malicioso.

4.3.1. Caso não haja confirmação de código malicioso, a contratada deverá enviar relatório técnico da análise do(s) arquivo(s) para o correio eletrônico seseg.cenin@camara.gov.br em até 15 (quinze) dias, contados da data de submissão do(s) arquivo(s).

4.4. A inobservância das obrigações previstas neste anexo poderá implicar aplicação de multa, conforme Anexo n. 8 deste Edital.

5- DA ATUALIZAÇÃO

5.1. A contratada fica obrigada a solucionar, sem custos, eventuais problemas relativos a defeitos ("*bugs*"), bem como a fornecer quaisquer correções ("*patches*") e atualizações disponibilizadas pelo fabricante da solução durante o período de garantia.

5.2. Para os efeitos da exigência anterior, entende-se como atualização, o provimento de toda e qualquer evolução, incluindo correções, "*updates*", "*service packs*", novas "*releases*", "*builds*" e funcionalidades, bem como o provimento de "*upgrades*" englobando, inclusive, versões não sucessivas e de novos produtos que substituam a solução em caso de descontinuidade, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 6

PREGÃO ELETRÔNICO N. 52/10

MODELO COMPLETO DA PROPOSTA

(Anexo disponível em documento WORD (.doc) para download na página http://www2.camara.gov.br/licitacoes/editais/pregaoeletronico.html).

PREGÃO ELETRÔNICO N. 52/10

OBJETO: prestação de serviços de implantação (licenciamento, capacitação operacional, instalação, configuração e ativação) e manutenção, que compreende garantia de funcionamento (suporte técnico) e garantia de atualização de solução de segurança de estações de trabalho (*Endpoints*) e servidores de rede pelo período de vinte e quatro meses.

EMPRESA: _____
CNPJ: _____
ENDEREÇO: _____
FONE/FAX: _____
ENDEREÇO ELETRÔNICO: _____
À
CÂMARA DOS DEPUTADOS

Em atendimento ao Edital do Pregão à epígrafe, apresentamos a seguinte proposta de preços:

ITEM	DESCRIÇÃO	MARCA (*)	UN.	QUANT.	PREÇO UNITÁRIO R$	PREÇO TOTAL (A) R$	PREÇO MENSAL R$ = (A)/Quant. de meses
Único	**Licenciamento, instalação, configuração, ativação e garantia de funcionamento e atualização de solução de segurança de estações de trabalho (Endpoints) e servidores de rede, incluindo capacitação operacional.**						
1.1	Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)		liç	1800			--------
1.2	Funcionalidade de controle de acesso à rede local de computadores		liç	7500			--------
1.3	Funcionalidade de criptografia de discos rígidos de estações de trabalho		liç	600			--------
1.4	Funcionalidade de controle de acesso de dispositivos às portas de comunicação de estações		liç	7700			--------

ITEM	DESCRIÇÃO	MARCA (*)	UN.	QUANT.	PREÇO UNITÁRIO R$	PREÇO TOTAL (A) R$	PREÇO MENSAL R$ = (A)/Quant. de meses
	e servidores de rede						
1.5	Funcionalidade de proteção contra códigos maliciosos no Exchange Server 2003		**(**)**	**(**)**	**(**)**	**(**)**	--------
1.6	Instalação e configuração (Subitens 1.1 a 1.5)	---	sv	1			--------
1.7	Capacitação operacional	---	sv	1			--------
1.8	Garantia de funcionamento e de atualização da solução por vinte e quatro meses (Subitens 1.1 a 1.5)	---	sv	1			(A)/24
1.9	Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)		liç	5900			--------
1.10	Instalação e configuração (Subitem 1.9)	---	sv	1			--------
1.11	Garantia de funcionamento e de atualização da solução por vinte e um meses (Subitem 1.9)	---	sv	1			(A)/21
Preço Total do item único R$						**(***)**	--------
Preço total do item único por extenso:							

(*) Indicar marca, modelo, tipo, configuração, versão, pacote, dos componentes e subcomponentes, onde couber.

(**) O subitem 1.5 poderá ser cotado de acordo com as seguintes opções:

- **12.100 (doze mil e cem) caixas postais eletrônicas ou**

- **6 (seis) computadores servidores.**

A licitante deverá preencher os campos referentes ao item 1.5 da planilha de preços, indicando a unidade e o quantitativo a serem cotados, de acordo com a forma de comercialização das licenças pela licitante, com os referentes preços unitário e total.

(***) OBS.: O valor indicado nesta célula é o valor que deve ser considerado no envio da Proposta Eletrônica (Anexo n. 7).

PRAZO DE VALIDADE DA PROPOSTA: _____ (por extenso) dias (observar o disposto na alínea "c" do item 7.2).

PRAZOS DE ENTREGA DOS COMPONENTES E EXECUÇÃO DOS SERVIÇOS, CONFORME CRONOGRAMA DE ENCADEAMENTO DAS FASES DISPOSTO NO ANEXO N. 4 DO EDITAL.

PRAZO DE GARANTIA DE FUNCIONAMENTO E ATUALIZAÇÃO REFERENTE AOS SUBITENS 1.1 A 1.5 DO OBJETO DA LICITAÇÃO CONTIDO NO ANEXO N. 1**:** _____ (por extenso) meses (observar o disposto na alínea "e.1" do item 7.2)**.**

PRAZO DE GARANTIA DE FUNCIONAMENTO E ATUALIZAÇÃO REFERENTE AO SUBITEM 1.9 DO OBJETO DA LICITAÇÃO CONTIDO NO ANEXO N. 1**:** _____ (por extenso) meses (observar o disposto na alínea "e.2" do item 7.2)**.**

Declaramos que os subitens constantes dessa planilha correspondem exatamente às especificações descritas no Anexo n. 2 deste Edital, às quais aderimos formalmente.

Declaramos conhecer e aceitar todas as exigências do Edital e dos anexos da presente licitação.

Declaramos que conhecemos a natureza e as condições de execução dos serviços referentes ao objeto desta licitação.

Declaramos que anexamos a esta proposta o detalhamento da forma de licenciamento de cada componente da solução de segurança das estações de trabalho (Endpoints) e servidores de rede.

Comprovação da conformidade técnica

Caso a comprovação da especificação esteja distribuída por vários manuais, listar o nome dos manuais e atribuir um número a cada um. Na coluna "Manual/Página", atribuir um número a cada manual e informar esse e a(s) página(s) correspondente(s).

Especificação	Nº Manual/ Pág	Conf
Gerenciamento via console(s) central(is) de um mesmo fabricante.		
Máximo de três consoles centrais de gerenciamento.		
Alta disponibilidade por meio de balanceamento de carga em: - Dois ou mais consoles centrais de gerenciamento em execução em máquinas diferentes. - Dois ou mais consoles centrais de gerenciamento funcionando no modo de *cluster* ativo-ativo ou ativo-passivo.		
Armazenamento centralizado de registros (*logs*);		
Download automático de atualizações ou por comando dos administradores a partir do site do fabricante da solução.		
Mecanismo para desinstalação de atualizações de forma centralizada.		
Distribuição automática de políticas e atualizações via rede ou por comando pelos administradores.		
Aplicação de políticas segundo os critérios de: Todos os agentes; Grupos de agentes ou estações; Agente ou estação específica.		
Personalização das notificações aos usuários para português (Brasil).		
Gerência de todas as funcionalidades da solução, incluindo a gerência remota de todas as funcionalidades do(s) agente(s) local(is), por meio de interface gráfica.		
Interface gráfica para a geração de relatórios sobre o funcionamento da solução e sobre os dados coletados por meio do(s) agente(s).		
Definição de grupos de usuários e equipamentos a serem utilizados nas políticas.		
Integração com o Microsoft Active Directory 2003 e superior.		
Capacidade de importação e sincronização de usuário, grupos de usuários,		

Especificação	Nº Manual/ Pág	Conf
máquinas e grupos de máquinas presentes no Active Directory.		
Granularidade para atribuir níveis de acesso de leitura ou controle total das funcionalidades da solução de *Endpoint.* aos usuários do(s) console(s).		
Sistema de auditoria para registrar todas as ações executadas pelos usuários do(s) console(s) de gerenciamento.		
Controle dos intervalos de comunicação entre o(s) console(s) de gerenciamento e o(s) agente(s) local(is)		
Gerar alertas e relatórios contendo a lista de máquinas desatualizadas.		
Definir prazo mínimo para que uma máquina seja considerada desatualizada		
Agente(s) local(is):		
Compatibilidade com Microsoft Windows Vista/XP/2000 Professional em português e Microsoft Windows 2000 Server, Windows Server 2003 e superiores em inglês.		
Instalação e desinstalação de forma automática por meio do(s): console(s) de gerenciamento ou *prompt* de comando (*shell*) ou criação de pacote de instalação no formato .msi ou .exe a ser usado por sistema especializado na distribuição de software.		
Operação *off-line* quando não for possível entrar em contato com o(s) console(s) de gerenciamento.		
Continuar operando com a última política recebida enquanto não for restabelecida a comunicação com o(s) console(s) de gerenciamento.		
Permitir o uso de políticas diferentes quando a estação estiver conectada à rede interna (com acesso ao domínio Active Directory) e quanto estiver conectada a outras redes.		

Especificação - AntiMalware	Nº Manual/ Pág	Conf
Prover atualizações, no máximo, diárias das definições de *malware* utilizadas. As atualizações deverão ser obtidas pelo(s) console(s) de gerenciamento e distribuídas ao(s) agente(s) local(is) automaticamente.		
Implementar as seguintes formas de varredura contra *malwares* em memória RAM, arquivos, *Registry* e *cookies*:		
Varredura agendada com definição de horários para a verificação das máquinas.		
Habilitação e desabilitação dos agendamentos.		
Agendamentos diários, semanais, ao iniciar o sistema operacional e no logon do usuário.		
Varredura tempestiva em uma estação ou grupo de estações, com comando por meio do(s) console(s) de gerenciamento.		
Varredura em tempo real (*on-access scanner*).		
Varredura heurística para:Detectar arquivos executáveis que tenham código malicioso ou programas potencialmente indesejados; Procurar vírus desconhecidos.		
Configuração de um período de tempo máximo para as varreduras e cancelamento automático em caso de expiração.		
Execução de varreduras por linha de comando ou a partir de arquivos de *batch* ou scripts.		
Opções para quando uma ameaça for encontrada:		
Ação principal: “Limpar automaticamente”, “Negar acesso ao arquivo” ou “Excluir automaticamente” ou ações similares.		
Ação secundária: “Negar acesso ao arquivo”, “Excluir automaticamente”, “Mover arquivo para área de quarentena” ou “Continuar varredura” ou ações similares.		
Formas de classificação e detecção de programas indesejados:		
Vírus, *spyware*, *adware, worms*, discadores, capturadores de digitação (*Keyloggers*), ferramentas de administração remota.		
Detecção baseada em nomes de arquivos definidos pelo administrador por meio do(s) console(s) de gerenciamento.		
Excluir da varredura arquivos, diretórios, chaves de *Registry* ou *cookies* específicos definidos pelo administrador.		
Opções de exame para todos os tipos de varredura:Todos os arquivos; Extensões		

Especificação - AntiMalware	**Nº Manual/ Pág**	**Conf**
pré-definidas contidas em lista inicial de extensões perigosas e permitir a inclusão de outras extensões.		
Cadastrar extensões que não devem ser verificadas.		
Verificar arquivos compactados nos formatos mais utilizados em nível configurado pelo administrador da solução de Endpoint e codificados MIME.		
Configurar tempo máximo de varredura para esses arquivos.		
Varredura de arquivos aninhados (*nested files*), ou seja, verificar arquivos compactados que estejam dentro de outros arquivos compactados.		
Configuração do nível máximo de aninhamento de compactadores e ação a ser executada.		
Verificar arquivos de macro e verificar macros em arquivos de programas de escritório (*Microsoft Office*, *BrOffice* e similares).		
Definição do uso máximo de CPU pelo(s) agente(s) local(is) para cada varredura agendada.		
Manutenção de registros (logs) de todas as ações executadas.		
Impedir a execução de scripts e programas nas pastas de armazenamento temporário (por exemplo, c:\temp, pastas *temp* privativas dos usuários, "Temporary Internet files").		
Classificação "*Advanced*" nos testes do AV-comparatives (www.av-comparatives.org) ou ter sido aprovado em um dos dois últimos testes VB100 da Virus Bulletin (www.virusbtn.com).		
Em caso de "falsos positivos", última assinatura de malware deverá ser reinstalada.		

Especificação - Firewall pessoal	**Nº Manual/ Pág**	**Conf.**
Ativação ou desativação do firewall por máquinas ou grupos de máquinas.		
Importar as configurações de firewall de uma estação de trabalho e aplicá-la a outra estação ou a um grupo de estações.		
Criação, alteração e exclusão de lista autorizada (white list) e não autorizada (black list) de execução de programas. As aplicações da lista autorizada sempre terão permissão de execução nas estações. As aplicações da lista não autorizada nunca terão permissão de execução nas estações.		
Criação, alteração e exclusão de listas autorizada (white list) e não autorizada (black list) de endereços IP. Os endereços da lista autorizada sempre terão permissão de acesso via rede às estações. Os endereços da lista não autorizada nunca terão permissão de acesso via rede às estações.		
Criação e aplicação remota de políticas distintas de firewall a grupos diferentes de máquinas.		
Implementar política que permita que apenas uma interface de rede esteja ativa em cada estação.		
Recursos para impedir o desligamento das políticas de firewall por atacantes ou malware.		
Filtragem por tipo de tráfego, aplicação que envia ou recebe dados e assinaturas de ataques conhecidos.		
Por meio da interface gráfica do(s) console(s) de gerenciamento, o firewall deverá possuir os seguintes itens de configuração:		
Habilitar ou desabilitar detecção de intrusão;		
Exibir ou não mensagem de notificação de ataque;		
Quando estiver sob ataque:		
Habilitar ou não exibição de mensagem;		
Permitir envio de email aos administradores.		
Assinaturas de ataque de Port scan (UDP e TCP), Syn flood e PPTP buffer overflow.		
Regras baseadas em tipo de conexão, protocolos IP e não IP, direção do tráfego de rede, aplicação geradora do tráfego, serviço ou porta usada pelo computador, endereço IP usado no pacote.		
Recurso de duplicação de regras existentes.		
Níveis de proteção baixo, alto e personalizado		

Especificação - Host-Based Intrusion Prevention System – HIPS	**Nº Manual/ Pág**	**Conf.**
Regras baseadas em: Protocolos IP e não IP; Direção do tráfego (entrada, saída ou ambas);Tipo de conexão (rede ou sem fio); Aplicações que geraram o tráfego; Serviço ou porta usados pelo computador local;Serviço ou porta usados pelo computador remoto; Endereços IP de origem ou destino; Conteúdo dos pacotes.		
Modelos de políticas personalizáveis para aplicações e configurações mais usuais.		
Habilitar ou desabilitar as políticas em estações ou grupos de estações.		
Definição de políticas para permitir ou bloquear a execução de determinadas aplicações.		
Ações de registrar (*log*) ou impedir execução.		
Configuração de notificações de alerta por email.		
Tipos de bloqueio de execução: Execução de aplicação (criação de processo) e Anexação (*hook*) de código a um processo em execução.		
Criação de exceções às políticas (classificar aplicações como confiáveis).		
Assinaturas para proteção contra ataques de rede e atualização periódica.		

Especificação - *Network Access Control* – NAC	**Nº Manual/ Pág**	**Conf.**
Compatibilidade com 802.1x (via software ou hardware - appliances) ou Microsoft Network Access Protection (NAP)		
Bloquear ou colocar sob regime de quarentena os dispositivos que tentarem se conectar à rede da Câmara dos Deputados e não atenderem aos requisitos de segurança, impedindo o acesso à rede local e recursos compartilhados.		
Conformidade do dispositivo tentando conectar à rede da Câmara, tais como: versão da base de dados de malware, firewall configurado conforme as políticas corporativas e ativo, service packs e patches de segurança do sistema operacional atualizados.		
Identificar os sistemas não gerenciados (que não possuem o(s) agente(s) local(is) instalado(s)) e aplicar políticas específicas para esses sistemas.		
Definir tipos ou grupos de sistemas. Deverá permitir a definição de políticas de conformidade específicas para cada grupo ou tipo de sistema.		
Definição de níveis diferentes de acesso à rede, dependendo da violação da política de acesso que foi identificada.		
Configurações de máquinas ou grupos de máquinas isentos das políticas de NAC.		
Remediação automaticamente. A remediação deverá incluir todas as ações necessárias para deixar o sistema conforme a política aplicável.		
Funcionalidade de exibição de mensagens de não conformidade aos usuários, listando os problemas encontrados e procedimentos para restaurar o estado de conformidade da estação.		
Definição de quando avaliar a conformidade de sistemas por meio de varreduras:No início do sistema; Quando um sistema é reconectado à rede ou se houver mudança no estado do adaptador de rede; Quando o console do servidor NAC solicitar.		
Agendamento de varredura de clientes gerenciados pelo(s) console(s) de gerenciamento. A solução deve prover mecanismo para habilitar ou desabilitar o agendamento para grupos de máquinas definidas no(s) console(s) de gerenciamento.		
Mínimo, 2 (dois) modos de funcionamento (*enforcement*): Aplicar (*enforce*) a política, restringindo o acesso à rede; Apenas monitorar e registrar os casos de não conformidade.		
Exportação e importação de políticas de conformidade de *Endpoint.*		
Relatórios: Via console de gerenciamento, monitoração do acesso à rede (quantidade de máquinas em conformidade (*compliant*) com as políticas e em não conformidade.		

Especificação - Criptografia de discos rígidos	**Nº Manual/ Pág**	**Conf.**
Método que permita ao administrador recuperar acesso a dados criptografados de forma controlada e somente quando for necessário.		

Método de criptografia persistente, independentemente do sistema de arquivo destino (FAT, FAT32, NTFS).		
Suporte à criptografia de todo o disco rígido (ou de partições completas) com autenticação antes ou durante o pré-carregamento do sistema operacional.		
Implementar o algoritmo AES com chaves de 256 bits conforme o padrão FIPS 197.		
Suportar as recomendações do NIST SP800-111 (*Guide to Storage Encryption Technologies for End User Devices*).		
Padrão IEEE 1619.		
Uso de *tokens* ou *smart cards* com certificados digitais como mecanismo de autenticação.		

Especificação - Controle de dispositivos	**Nº Manual/ Pág**	**Conf.**
Controle de interfaces PCMCIA, USB 1.0, 1.1 e 2.0, Firewire, ATAPI, Serial (COM), Paralela, IrDA, SCSI, Bluetooth.		
Controle de d*rives* de disco, *p*en drives, dispositivos de imagem, adaptadores de vídeos, teclados, leitores de smart card, drives de CD-ROM/DVD, mouse e outros dispositivos apontadores, controladores de som, vídeo e jogos, drives de disquete, drives de fita e dispositivos de interface humana (HID), dispositivos ACPI específicos, PDAs (Palm, Windows e similares), controladores de cartão de memória.		
Modo de aprendizado para dispositivos que são específicos de um fabricante. O aprendizado deverá permitir que a solução passe reconhecer o dispositivo e possa gerenciá-lo.		
Granularidade para que alguns dispositivos específicos sejam permitidos, mesmo que a política geral os bloqueie. A solução deverá possibilitar aos administradores permitir o uso dos dispositivos com base em número de série, modelo e/ou fabricante.		
Aplicação de políticas específicas para grupos de máquinas e usuários definidos no Active Directory.		
Executar atualização de políticas quando usuário efetuar login.		
Manutenção das políticas mesmo que esteja desconectada da rede e sem acesso ao(s) console(s) de gerenciamento.		
Permissões de acesso: Leitura;Leitura e escrita;Bloqueio.		

Especificação - Antimalware para *Exchange Server* 2003 e superior	**Nº Manual/ Pág**	**Conf.**
Integrar gerenciamento de antimalware ao(s) console(s) de gerenciamento;		
Integração com *Active Directory da Microsoft*;		
Compatibilidade com as *APIs* de varredura de código malicioso da Microsoft listadas em http://support.microsoft.com/kb/823166;		
Atualização automática dos arquivos de assinatura de códigos maliciosos;		
Filtragem de mensagens eletrônicas de entrada e saída;		
Identificação de tipo de arquivo e capacidade de filtragem de busca e remoção de anexos e anexos aninhados em arquivos compactados;		
Recurso de gerenciamento de surtos de código malicioso baseado em regras;		
Aplicação políticas de grupo a usuários como exceção à política global;		
Alerta de descarte de mensagens infectadas por código malicioso;		
Registros (*logs*) consolidados no(s) console(s) de gerenciamento.		

N. Manual/ Pág.: número da página ou outra referência na documentação técnica apresentada pela licitante, na qual se possa comprovar o item em questão.
Conf.: será utilizado pelos técnicos do Centro de Informática para conferência da especificação técnica.

Brasília, de de 2010.

_____

Assinatura do representante legal da empresa

_____

Nome do representante legal da empresa

SOMENTE PARA A LICITANTE QUE HOUVER SE MANIFESTADO CONFORME DISPOSTO NO ITEM 5.2.1 DO EDITAL:

Declaramos, sob as penas da lei, que cumprimos os requisitos legais para a qualificação como microempresa/ empresa de pequeno porte e estamos aptos a usufruir do tratamento favorecido estabelecido nos artigos 42 a 48 da Lei Complementar n. 123, de 2006.

Brasília, de de 2010.

_____

Assinatura do representante legal da empresa

_____

Nome do representante legal da empresa

(SÓ ASSINAR SE ESTIVER HABILITADA A EXERCER O DIREITO DE PREFERÊNCIA REFERIDO ACIMA)

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

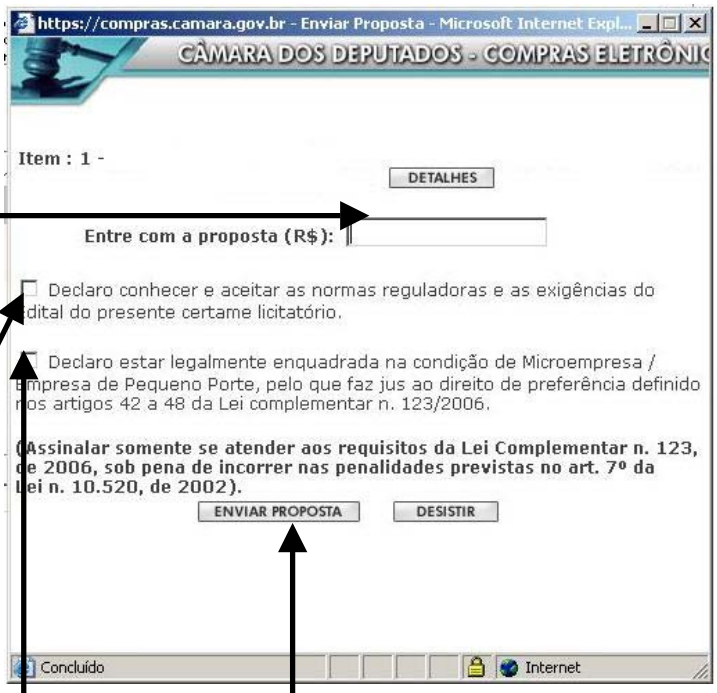
ANEXO N. 7

PREGÃO ELETRÔNICO N. 52/10

CÓPIA DO FORMULÁRIO ELETRÔNICO DE ENTRADA DOS DADOS DA PROPOSTA

Informe o **PREÇO TOTAL** oferecido para o item único.
NÃO DIGITE VÍRGULAS.
Exemplos:
a) se o valor é **R$ 1,45** digite **145**
b) se o valor é **R$ 10,00** digite **1000**

É necessário assinalar a declaração de que conhece e aceita as normas reguladoras e as exigências do Edital.



Após preencher o valor da proposta para o item e assinalar a declaração, clicar com o mouse sobre o botão “Enviar Proposta”.

Caso queira usufruir do tratamento favorecido estabelecido nos artigos 42 a 48 da Lei Complementar 123, de 2006, a licitante enquadrada como microempresa ou empresa de pequeno porte **deverá declarar**, por ocasião do encaminhamento da proposta e em campo próprio do sistema eletrônico, que atende aos requisitos previstos no artigo 3 da referida lei.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 8

PREGÃO ELETRÔNICO N. 52/10

TABELA DE MULTAS

Para efeito de aplicação de multas à contratada pela inobservância das obrigações descritas neste Edital, são atribuídos percentuais sobre o valor total do contrato, conforme tabela abaixo:

INFRAÇÃO	**PERCENTUAL**

Deixar de:

1. concluir as atividades da Fase 1 dentro do prazo estipulado e nas condições definidas no Edital, por dia de atraso 0,01%
2. concluir as atividades da Fase 2 dentro do prazo estipulado e nas condições do Anexo n. 4, por dia de atraso 0,02%
3. concluir as atividades da Fase 3 dentro do prazo estipulado e nas condições do Anexo n. 4, por dia de atraso 0,02%
4. concluir as atividades da Fase 4 dentro do prazo estipulado e nas condições do Anexo n. 4, por dia de atraso 0,02%
5. entregar relatório técnico, por dia de atraso 0,01%
6. atender às solicitações técnicas nos moldes e prazos mencionados no Anexo n. 5 deste Edital, aplicando-se multa de acordo com as seguintes regras:
   - 6.1. Crítica – Solução totalmente parada e deverá ser recolocada em funcionamento completo em até vinte e quatro horas. Multa por hora de atraso 0,05%
   - 6.2. Alta – Solução com funcionalidades importantes parcialmente paradas deverá ser recolocada em funcionamento em até dois dias. Multa, por dia de atraso 0,04%
   - 6.3. Média – Solução com erros ou problemas que causam impacto moderado no ambiente de produção deverá ser recolocada em funcionamento em até cinco dias. Multa por dia de atraso 0,03%
   - 6.4. Baixa – Solução com erros ou problemas que causam pouco impacto no ambiente de produção, bem como consultas técnicas, atualizações, implementação de novas funcionalidades e resolução de dúvidas em geral deverão ser resolvidas em até cinco dias. Multa, por dia de atraso 0,02%
   - 6.5. Preventiva/Evolutiva – consultas técnicas, atualizações, implementação de novas funcionalidades e resolução de dúvidas em geral deverão ser resolvidas em até quinze dias. Multa por dia de atraso 0,01%
7. comunicar a disponibilidade de novas versões dos softwares, nos termos do Anexo n. 5, por ocorrência 0,03%

8. identificar previamente, junto ao órgão fiscalizador, as pessoas com atribuição de execução de serviços pela contratada, por ocorrência 0,04%
9. cumprir instrução do órgão fiscalizador para execução dos serviços, ou qualquer outra exigência ou obrigação contratual ou legal, por ocorrência 0,03%
10. alocar técnico que possua certificação e o vínculo empregatício exigido, por ocorrência 0,05%
11. fornecer vacinas para detecção e remoção de código malicioso submetido pela Câmara, por dia 0,02%

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 9

PREGÃO ELETRÔNICO N. 52/10

MODELO DE ATESTADO DE CAPACIDADE TÉCNICA

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, para os devidos fins, que a empresa ....., estabelecida ....., forneceu satisfatoriamente, no que diz respeito à venda, ao prazo de entrega e à assistência técnica, o(s) produto(s) e serviços abaixo relacionado(s). Acrescentamos que os produtos apresentam (ou apresentaram) desempenho operacional satisfatório.

Atestamos também que o número de estações de trabalho protegido pela solução *Endpoint* citada abaixo é de .....(valor por extenso) e que o número de servidores computadores protegidos é de .....(valor por extenso).

Número mínimo de estações: 1.500 (mil e quinhentas)

Número mínimo de servidores computadores: 20 (vinte)

Data de Licenciamento	**Funcionalidades da solução *Endpoint***
___/___/___	Software *antimalware* *Firewall* pessoal Prevenção de intrusão para máquina (“H*ost-Based Intrusion Prevention* – HIPS”) Controle de dispositivos (portas de comunicação)

Data de término	**Serviços executados**
___/___/___ ___/___/___	- Implantação - suporte técnico

_____

(local e data)

_____

(assinatura do cliente, com o nome digitado, cargo que ocupa, telefones de contato)

Observações:
Devido à complexidade de planejamento, configuração e implementação dessa solução, apenas serão aceitos atestados de produtos e serviços que contenham, no mínimo, as funcionalidades descritas neste Edital.

O(s) atestado(s) dever(á)ão ser apresentado(s) em papel timbrado do cliente.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 10

PREGÃO ELETRÔNICO N. 52/10

MODELO DE DECLARAÇÃO DE ESTRUTURA FÍSICA DE SUPORTE TÉCNICO

DECLARAÇÃO DE ESTRUTURA FÍSICA DE SUPORTE TÉCNICO

Declaramos, para os devidos fins, que possuímos estrutura física de suporte técnico no Brasil, situado a _____, <cidade>, <Estado>, <endereço eletrônico>, <telefone>, <fax>.

(nome da licitante)
CNPJ xx.xxx.xxx/xxxx-xx,
Telefone de contato do local indicado

Data: __/___/____

Nome do representante legal: _____

Assinatura do representante legal: _____

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 11

PREGÃO ELETRÔNICO N. 52/10

PROVA DE CONCEITO

1.1. É condição para classificação, a obtenção da aprovação da solução oferecida, por meio da realização da Prova de Conceito constante deste anexo.

1.2. Serão informadas a data e a hora em que se fará a comunicação, por via eletrônica, do resultado da Prova de Conceito realizada.

a) Com o objetivo de agilizar a configuração da solução de Endpoint, é facultado à licitante trazer os softwares instalados em máquina virtual, preferencialmente, VMWare Server 1.0, ou
b) A licitante deverá enviar documento informando a quantidade e especificação técnica dos computadores servidores que serão necessários para a prova de conceito.
c) A licitante deverá instalar e configurar o software em máquina(s) indicadas pelo Cenin e que atendam aos requisitos de hardware indicados pelo fabricante da solução de *Endpoint* e servidores computadores. **O prazo para essa tarefa é de até dez dias, contados do anúncio do pregoeiro confirmando a adequação da documentação e da proposta apresentadas pela licitante.**
d) Depois da instalação do software e outros procedimentos necessários ao pleno funcionamento, o(s) console(s) de gerenciamento deverá(ão) ser acionado(s) para início da prova de conceito. **O prazo para conclusão da prova de conceito por parte do órgão fiscalizador é de dez dias, contados da instalação citada na alínea anterior.**
e) Outros testes, baseados nas especificações técnicas, poderão ser solicitados durante a Prova de Conceito.

Características a serem comprovadas	(S/N)
1) Console(s) de gerenciamento e configurações de antimalware:	-------
• Configurações gerais: - Personalização do(s) console(s) de gerenciamento; Definir administradores (importados do AD) da solução *Endpoint* (permissões de acesso especiais a usuários e grupos importados do AD de somente leitura, leitura/escrita, controle completo às funcionalidades da solução, habilitação de auditoria, etc.); -Acesso a site para baixar atualizações; - Personalização de notificações que usuários lerão para português (Brasil); - Criação de políticas para os testes;- Configurar relatórios pertinentes às ações executadas; - - Agente(s) [Intervalos de comunicação entre o(s) agente(s) e o(s) console(s) de gerenciamento, operação com a última política recebida quando não houver comunicação com o(s) console(s) e quando estiver conectado a outras redes]; - Configuração de alertas básicos para todas as funcionalidades da solução;	
• Descobrir (*discovery*) sessenta máquinas na rede local usando recursos de varredura da solução.	

Características a serem comprovadas	(S/N)
• Importar vinte máquinas do Active Directory (grupo WSUS), incluindo algumas máquinas da Cainf.	
• Dos números acima, instalar o agente de gerenciamento em algumas máquinas de forma automática (sem interação com o usuário)	
• Desinstalação do antivírus atual em algumas máquinas da CAINF.	
• Instalar solução *Endpoint* em algumas máquinas da CAINF.	
• Exibir no console o registro (*log*) das máquinas (instalação com sucesso, falha, outros).	
• Determinar e demonstrar intervalo de comunicação entre agentes e servidor em dez minutos para aplicação ou reaplicação das políticas criadas.	
• Criar cinco grupos com vinte máquinas em cada grupo. • Incluir as máquinas da CAINF no grupo 5.	
• Para cada grupo, definir varredura com base nos nomes dos arquivo e busca nas unidades locais de disco rígido.	
Configurar as seguintes políticas: Para todos os grupos: I) Habilitar *log* da varredura. II) Caso encontre programas indesejados, a ação primária é 'Limpar arquivos' III) Excluir pasta “Radmin” da varredura. IV) A varredura deve ser feita apenas no momento de gravação de arquivos na mídia. V) Varredura emergencial: Todos os arquivos, habilitar heurística, 50% de uso de CPU, detectar programas indesejados. VI) Atualização automática: Todos os dias, horário a ser definido. VII) Atualização de engine: Semanalmente, horário a ser definido. VIII) Atualizar antimalware: Na iniciação do sistema operacional.	
- Implementar cinco varreduras agendadas contra malware: Grupo 1: Início às 12h30, semanalmente às terças. Ativar seleção aleatória de início em 5 minutos. Modo de varredura padrão. Excluir da detecção na pasta Windows, todas as subpastas de desinstalação de patches. Verificar macros em todos os arquivos. Habilitar heurística. Utilização do sistema: 20%. Se ação primária falhar, a ação secundária é “Continuar varredura”. Grupo 2: Início às 13h, semanalmente às quartas. Modo de varredura de todos os arquivos. Excluir da detecção pasta *C:\WINDOWS\system32*, subpasta *dllcache*. Não habilitar heurística. Utilização do sistema: 10% Grupo 3: Início às 13h30, semanalmente às quartas, ativar seleção aleatória de início em 10 minutos, modo de varredura de todos os arquivos. Excluir da detecção	

Características a serem comprovadas	(S/N)
pasta C:\Arquivos de programas\Internet Explorer. Habilitar heurística. Utilização do sistema: 30%. Executar tarefa novamente se for perdida e adiar execução por 15 minutos. Grupo 4: Início às 13h30, semanalmente às quintas, modo de varredura de todos os arquivos. Excluir da detecção pasta *C:\Documents and Settings\Default User*. Habilitar heurística. Utilização do sistema: 30%. Cancelar varredura caso demore mais de 120 minutos. Grupo 5: Início às 10h às segundas e 12h30 às quintas, ativar seleção aleatória de início em 15 minutos, modo de varredura padrão, habilitar heurística. Excluir da detecção pastas *C:*.log* e *C:*.tmp*. Verificar arquivos compactados. Utilização do sistema: 20%. Se ação primária falhar, a ação secundária é solicitar ação. Em solicitar ação, habilitar opção "Excluir". Cancelar varredura caso demore mais de 40 minutos. Executar tarefa novamente se for perdida e adiar execução por 30 minutos.	
Cancelar varredura agendada para o grupo 5.	
Exibir no console de gerenciamento o registro (*log*) das ações executadas pelo(s) agente(s) nas estações.	
Por meio do console de gerenciamento, solução deverá comprovar a freqüência de atualização das definições de softwares maliciosos, no máximo, a cada 24 (vinte e quatro) horas.	
Nas máquinas do grupo 5, implementar todas as configurações necessárias para reforçar a segurança em caso de epidemia de malware.	

Características a serem comprovadas	(S/N)
2) Firewall pessoal	-------
Todos os testes deverão ser feitos no grupo 5 (CAINF), usando o console de gerenciamento.	-------
Nos grupos 1 a 4, ativar o *firewall* no modo de somente registro (log)	
Ativar modo de aprendizado (*learn mode*) do *firewall* no grupo 5.	
Importar os logs do *firewall* do grupo 5 e extrair as regras mais comuns.	
Exportar as regras para o grupo 5.	
Criar e reforçar política de apenas uma *interface* de rede ativa.	
Configurar *firewall* para cadastrar três subredes como confiáveis	
No console, criar duas listas (*white list* e *black list*) e distribuir as listas em dois grupos de máquinas.	
Registrar, em *log*, data e hora, tipo de evento, tipos de aplicação dos pacotes que foram bloqueados e permitidos.	
Criar filtro para exibir tráfego de entrada, aplicação navegador Internet	

Características a serem comprovadas	(S/N)
Criar regra com nome “Block MSN”. Protocolo:IP-TCP. Direção: saída. Escolher uma aplicação via Windows Explorer (msmsgs.exe). Serviço local: *any*. Remote service: *any* .	
No console de gerenciamento, exibir informação que a política de *firewall* está ativa para as máquinas do grupo 5.	
Características a serem comprovadas	(S/N)
3) *Host Based Intrusion Prevention System* (HIPS)	-------
Criar regras baseadas em protocolo IP e não IP, direção do tráfego, conexão (rede cabeada ou rede sem fio), aplicações que geraram o tráfego, serviço ou porta no computador local e remoto.	
Comprovar existência de modo de aprendizado da solução.	
Exibir modelos prontos para aplicações mais comuns e configurações do sistema (serviços que exigem conectividade. Ex: lsaas.exe	
Configurar regras para monitoração de aplicação (*Firefox*) e bloquear *Internet Explorer* de ser executado.	
Comprovar geração de notificações de alerta por *email* e *traps* SNMP	
Comprovar no console de gerenciamento o recebimento dos registros efetuados pelos agentes.	
Comprovar bloqueio de programas na criação e quando for solicitada anexação (hook) a outra(s) aplicação (ões).	
Comprovar que solução possui recurso de configurar exceções às regras de assinaturas ou qualificar aplicações como confiáveis.	
Comprovar que solução consegue prover proteção contra ataques de rede.	

Características a serem comprovadas	(S/N)
4) *Network Access Control* - NAC	--------
Criar regra que bloqueie ou crie quarentena para dispositivos que tentam acessar o domínio que tenha antivírus desatualizado e patches de segurança não aplicados.	
Executar serviço de detecção de máquinas não gerenciáveis.	
Configurar máquinas que não foram aprovadas para remediação automaticamente.	
Criar três definições para avaliar a conformidade das estações por meio de varreduras: No início do sistema operacional, quando for reconectado à rede ou mudanças no adaptador de rede e ao comando do console de gerenciamento.	
Configurar mensagem de não conformidade aos usuários, listar problemas encontrados e ações para resolvê-los.	
Criar dois modos de *enforcement* : aplicar e monitorar.	
Exportar e importar políticas de conformidade	

Características a serem comprovadas	(S/N)
5) Prevenção ao vazamento de dados corporativos (Data Loss Prevention)	
A solução deverá possuir funcionalidade de *Data Loss Prevention* ou prover integração com as principais ferramentas de DLP do mercado.	

Características a serem comprovadas	(S/N)
6) Criptografia de discos rígidos	---
Prover suporte a métodos que permitam que o administrador tenha acesso à criptografia de forma controlada e somente quando for necessário.	
Deverá oferecer suporte à criptografia de todo o disco rígido (ou de partições completas) com autenticação antes ou durante o pré-carregamento do sistema operacional.	
Em uma máquina da CAINF, habilitar a criptografia de todo o disco rígido.	

Características a serem comprovadas	(S/N)
7) Controle de dispositivos	---
Todos os testes deverão ser feitos no grupo 5 (CAINF).	
Todas as configurações executadas abaixo deverão reportar registros (logs) ao console.	
Estabelecer comunicação periódica entre o agente e o console em 10 minutos.	
Importar usuários e máquinas do *MS Active Directory* para criação de políticas diferenciadas:	
Criar grupo com 5 máquinas da Cainf para impedir o uso de dispositivos *Bluetooth*.	
No grupo citado acima, liberar acesso de dispositivos apontadores (*mouse* e teclado).	
No grupo citado acima, configurar permissão de somente leitura para *pen drives* da marca *Sandisk*.	
Criar outro grupo com 5 máquinas da Cainf para impedir o uso de *pen drives*, *PDAs* e gravador de CD/DVD.	
No grupo citado acima, permitir que o grupo de usuários da Seseg tenha acesso aos dispositivos bloqueados.	
Criar novo grupo com 10 máquinas da Cainf para impedir o uso de *pen drives* da marca *Sandisk*.	

Características a serem comprovadas	(S/N)
Em um notebook, bloquear o uso do *PCMCIA*	
Criar política para que o grupo Seger possa utilizar *pen drives* via USB.	
Depois, configurar o grupo Seger para que não possa utilizar o gravador de CD/DVD.	
Efetuar *logoff* e *login* de usuário do grupo Seger para comprovar atualização da política.	
Desconectar uma máquina do grupo de teste, para comprovar manutenção da política.	

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 12

PREGÃO ELETRÔNICO N. 52/10

MODELO DO TERMO DE CONFIDENCIALIDADE

T E R M O D E C O N F I D E N C I A L I D A D E

_____, pessoa jurídica de direito privado, com sede na cidade de _____, Estado de _____, inscrita no CNPJ sob o n. _____, doravante referida como "**empresa**", representada pelo Sr(a). _____, RG _____ e CPF _____, doravante referido como "**representante**", concorda com os termos abaixo, relativos às condições de demonstração de produtos e serviços do ambiente da Câmara dos Deputados:

1. Sigilo de informações

A empresa, por manifestação de seu representante, concorda em não divulgar, por qualquer forma ou meio, quaisquer informações fornecidas pela Câmara dos Deputados ou obtidas pela empresa para fins de elaboração de proposta para participação em licitação, referente ao Pregão Eletrônico n. 52/10.

2. Ausência de Vínculo

O estabelecimento do presente "Termo de Confidencialidade" não configura qualquer compromisso nem vínculo financeiro ou de aquisição futura entre a Câmara dos Deputados e a empresa.
Os termos do presente "Termo de Confidencialidade" não compõem nem afetam qualquer interação ou contratação futura por parte da Câmara dos Deputados com a empresa.

Brasília, ____ de _____de 2010.

Representante Legal da Empresa	**Representante CENIN** Seção de Segurança de Rede Ponto: _____

Brasília, 11 de março de 2010.
José Martinichen Filho
Pregoeiro

ANEXO N. 13

PREGÃO ELETRÔNICO N. 52/10

GLOSSÁRIO

Adwares
É qualquer programa que automaticamente executa, mostra ou baixa publicidade para o computador enquanto uma aplicação é instalada ou executada, sem que seja necessária a autorização ou intervenção do usuário. Os *adwares* são conhecidos por trazerem para a tela do usuário algum tipo de propaganda. Costuma-se incluir os *adwares* à classe dos *spywares*, pois assemelham-se na sua forma de infecção e desinstalação. Sob a óptica da segurança, são tratados como se fossem um subgrupo dos *spywares*. Geralmente desenvolvidos por firmas comerciais, é comum que os *adwares* venham embutidos em diversos software do tipo *shareware* (de demonstração), com a autorização de seus autores, sendo que a versão comercial do software normalmente inibe a exibição de anúncios comerciais.

Bots
Um *bot* (contração de ro*bot*), é um utilitário concebido para simular ações humanas, em geral numa taxa muito mais elevada do que seria possível para um editor humano sozinho, ou seja, é uma forma automatizada de execução de uma determinada tarefa. Este tipo de programa de computador pode ter diversos usos, entre eles: ataques de DDoS, *downloaders* que ocupam toda a largura de banda dos *links* de comunicação, ataques coordenados do tipo *Botnet*/zumbis etc.

Cavalo de Tróia (*Trojan Horse*)
É um programa que age como a lenda do Cavalo de Tróia, entrando no computador e liberando uma porta para a ação de um possível invasor. Esse tipo de malware é instalado de forma sub-reptícia, sem que o usuário tenha consciência de sua instalação. Diferem-se dos vírus por não criarem réplicas de si próprios nem se autodisseminarem.

CoBit 4.1 - framework de gestão de Tecnologia da Informação e Comunicação
CoBit é o acrônimo para o título em inglês "*Control Objectives for Information and Related Technology*", ou, em português, Objetivos de Controle pata Tecnologia da Informação e Correlatas. A publicação do CobiT está em sua quarta edição, e é editada pelo IT Governance Institute – ITGI, ligado à instituição americana Information Systems Audit and Control Association – ISACA, cujas iniciativas são voltadas a prover aconselhamento acerca do controle, governança, auditoria e validação de sistemas de informação. A descrição do *framework* CobiT, constante das publicações do IT Governance Institute – ITGI, o apresenta como um *framework* de apoio à governança e controle que é estruturado em três níveis: domínios, processos e tarefas ou atividades. Os domínios agrupam os processos de acordo com a natureza desses, os quais, por sua vez, agrupam tarefas ou atividades às quais estão associados objetivos de controle. O CobitT distingue quatro domínios: 1) *Planejamento e organização*: Engloba os processos relativos à definição de estratégias e táticas, com ênfase na identificação das formas com que a TI

pode contribuir para o alcance dos objetivos de negócio. 2) *Aquisição e implementação*: Trata dos processos de implementação da estratégia de TI, por meio do levantamento das soluções necessárias, seguido de sua implementação e integração aos processos de negócio, seja por meio de desenvolvimento interno ou por aquisição de soluções de terceiros. 3) *Entrega e suporte:* Agrupa os processos relativos á execução e prestação dos serviços, que inclui a entrega de serviços, gestão da continuidade e da segurança, suporte aos usuários, gerenciamento dos dados, dos equipamentos e das instalações físicas. 4) *Monitoração e Avaliação*: Os processos deste domínio tratam da mensuração da performance, da monitoração dos controles internos, da avaliação da aderência a padrões, posto que todo processo de TI deve ser checado periodicamente quanto ao atendimento aos requisitos de controle de qualidade. Nesses domínios enquadram-se 34 processos, que se desdobram em 210 objetivos de controle, para os quais são definidos os objetivos a serem atingidos e as métricas para verificação do atingimento dos objetivos e mensuração da performance. Para isso são estabelecidos indicadores-chave de objetivo (*Key Goal Indicators*, ou KGI) e indicadores-chave de performance (*Key Performance Indicators*, ou KPI). São definidas também as responsabilidades e a atribuição das pessoas em relação a uma dada atividade ou tarefa. O CobiT agrega ainda um modelo de maturidade que permite mensurar o grau de maturidade para cada objetivo de controle definido.

Denial of Services (DoS)
Nos ataques de negação de serviço (DoS -- *Denial of Service*) o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet. Exemplos deste tipo de ataque são:
gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo.
gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível.
tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários a suas caixas de correio no servidor de *email* ou ao servidor *Web*.

Firewall
É o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

Gateway
Um *gateway*, ou porta de ligação, é uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos. Exemplos de *gateway* podem ser os roteadores e *firewalls*, já que ambos servem de intermediários entre o utilizador e a rede. Caracteriza-se por estar habitualmente posicionado na **periferia ou borda** da rede, ou seja, nos pontos de interconexão entre diferentes redes.

HIPS (*Host-Based Intrusion Prevention System, Host-Based IPS*)
Trata-se de um IPS (*Intrusion Prevention System*, ou sistema de prevenção de intrusão) residente em um IP específico, ou seja, em um determinado computador, em contraposição aos IPS's tradicionais, normalmente posicionados na borda da rede. É um programa de computador de detecção e prevenção baseado na estação que protege

recursos do sistema operacional e aplicações de ataques internos e externos. Complementa as técnicas tradicionais de detecção de *malware* pelos antivírus, os quais costumam empregar heurística e assinaturas (*fingerprint*), pouco eficiente quando se trata de um vírus novo desconhecido. Os HIPS's analisam o estado atual e o comportamento do computador visando prevenir a execução de ações maliciosas por parte de softwares ou atacantes mal-intencionados ou malcomportados.

ISO (*International Organization for Standardization) 17799/27002/270005- Normas que tratam do código de prática para a gestão da segurança da informação*

Malware (*Malicious software)*
O termo *malware* é proveniente da contração, em inglês, da expressão "software malicioso". Refere-se a qualquer tipo de código de computador destinado a se infiltrar em um sistema de computador alheio de forma ilícita e sem prévio consentimento, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). São considerados malware todo tipo de vírus de computador, *spyware, worms, trojan horses, adware, bots, rootkits, backdoors, dialers* (discadores), *screen scrapers* (capturadores de dados de tela)*, keyloggers* (capturadores de teclado) etc.

NAC – *Network Access Control*
É um sistema de computador que impõe políticas de segurança às estações de trabalho para verificar se o usuário e o computador estão em conformidade com essa política de segurança, estabelecida pelo administrador de rede, para concessão de permissão para conectar-se à rede local. O NAC é um elemento importante da arquitetura de segurança de *Endpoint*, pois promove a aglutinação das estratégias de proteção de estação (antivírus, HIPS), autenticação de usuários e máquinas, além de garantir a aderência às políticas de segurança de rede.

Patches
O nome vem da palavra em inglês para "remendo". São programas concebidos para efetuarem manutenção corretiva, preventiva ou evolutiva de outros códigos de programas com problemas de performance, estabilidade ou segurança, ou para implementação de aprimoramentos em softwares pré-existentes.

Proxy
O serviço de *proxy* ("procurador", em português) é implementado por um servidor por intermédio do qual requisições são repassadas a outros servidores capazes de atendê-las. Um *proxy* típico é o serviço de *web proxy*, que intermedeia as requisições de todas as estações da rede para a Internet, possibilitando o compartilhamento de um *link* Internet único, protegendo o acesso aos conteúdos externos e acelerando o tempo de resposta, por meio de um *cache* local das páginas estáticas externas mais frequentemente acessadas pelos clientes da rede interna.

Rootkits
Um rootkit é um *trojan* que busca se esconder de softwares de segurança e do usuário utilizando diversas técnicas avançadas de programação.

Spyware
Consiste em um programa automático de computador, que recolhe informações sobre o usuário, sobre seus costumes na Internet e transmite esta informação a uma entidade externa na Internet, sem o seu conhecimento e o seu consentimento.
Por outro lado, muitos vírus transportam *spywares*, que visam roubar certos dados confidenciais dos usuários. Furtam *logins* bancários, montam e enviam registros das atividades do usuário, roubam determinados arquivos ou outros documentos pessoais.

Vírus de computador
Um vírus de computador é um programa malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.

Worm
É um programa autorreplicante, semelhante a um vírus. Entretanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar. O *Worm* é um programa completo e não precisa de outro programa para se propagar.

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 14

PREGÃO ELETRÔNICO N. 52/10

ORÇAMENTO ESTIMADO

ITEM	DESCRIÇÃO	UN.	QUANT.	PREÇO UNITÁRIO R$	PREÇO TOTAL (A) R$	PREÇO MENSAL R$ = (A)/Quant. de meses
Único	**Licenciamento, instalação, configuração, ativação e garantia de funcionamento e atualização de solução de segurança de estações de trabalho (Endpoints) e servidores de rede, incluindo capacitação operacional.**					
1.1	Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)	liç	1800	61,88	111.384,00	---
1.2	Funcionalidade de controle de acesso à rede local de computadores	liç	7500	19,35	145.125,00	---
1.3	Funcionalidade de criptografia de discos rígidos de estações de trabalho	liç	600	120,50	72.300,00	---
1.4	Funcionalidade de controle de acesso de dispositivos às portas de comunicação de estações e servidores de rede	liç	7700	67,50	519.750,00	---
1.5	Funcionalidade de proteção contra códigos maliciosos no Exchange Server 2003	sv	1	15.037,50	15.037,50	---
1.6	Instalação e configuração (Subitens 1.1 a 1.5)	sv	1	105.975,00	105.975,00	---
1.7	Capacitação operacional	sv	1	29.000,00	29.000,00	---
1.8	Garantia de funcionamento e de atualização da solução por vinte e quatro meses (Subitens 1.1 a 1.5)	sv	1	36.968,35	36.968,35	1.540,35
1.9	Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)	liç	5900	61,88	365.092,00	---
1.10	Instalação e configuração (Subitem 1.9)	sv	1	11.775,00	11.775,00	---
1.11	Garantia de funcionamento e de atualização da solução por vinte e um meses (Subitem 1.9)	sv	1	17.544,24	17.544,24	835,44
				Preço Total do item único R$	**1.429.951,09**	---

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro

ANEXO N. 15

PREGÃO ELETRÔNICO N. 52/10

MINUTA DO CONTRATO

CONTRATO CELEBRADO ENTRE A CÂMARA DOS DEPUTADOS E A (ADJUDICATÁRIA) PARA PRESTAÇÃO DE SERVIÇOS DE IMPLANTAÇÃO E MANUTENÇÃO DE SOLUÇÃO DE SEGURANÇA DE ESTAÇÕES DE TRABALHO (ENDPOINTS) E SERVIDORES DE REDE PARA A CÂMARA DOS DEPUTADOS.

Ao(s) dia(s) do mês de de dois mil e dez, a CÂMARA DOS DEPUTADOS, situada na Praça dos Três Poderes, nesta Capital, inscrita no CNPJ sob o n. 00.530.352/0001-59, daqui por diante denominada CONTRATANTE, e neste ato representada por seu Diretor-GERAL, o senhor SERGIO SAMPAIO CONTREIRAS DE ALMEIDA, brasileiro, casado, residente e domiciliado em Brasília - DF, e a (ADJUDICATÁRIA), situada na (endereço e cidade), inscrita no CNPJ sob o n. , daqui por diante denominada CONTRATADA, e neste ato representada por seu (cargo na empresa), o senhor (nome e qualificação), residente e domiciliado em (cidade), perante as testemunhas que este subscrevem, acordam em celebrar o presente Contrato, em conformidade com o processo em referência, com as disposições contidas na Lei n. 8.666, de 21/06/93, e alterações posteriores, daqui por diante denominada simplesmente LEI, na Lei n. 10.520, de 17/07/02, no Regulamento dos Procedimentos Licitatórios da Câmara dos Deputados, aprovado pelo Ato da Mesa n. 80, de 07/06/01, publicado no D.O.U. de 05/07/01, doravante denominado simplesmente REGULAMENTO, e com o Edital do Pregão Eletrônico n. 52/10 e seus Anexos, observadas as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO

O objeto do presente Contrato é a prestação de serviços de implantação (licenciamento, capacitação operacional, instalação, configuração e ativação) e manutenção, que compreende garantia de funcionamento (suporte técnico) e garantia de atualização de solução de segurança de estações de trabalho (*Endpoints*) e servidores de rede pelo período de vinte e quatro meses, para a Câmara dos Deputados, de acordo com as especificações técnicas descritas no Anexo n. 2 ao Edital do Pregão Eletrônico n. 52/10 e demais exigências e condições expressas no referido Edital e em seus Anexos.

Parágrafo primeiro – Fazem parte do presente Contrato, para todos os efeitos:

a) Edital do Pregão Eletrônico n. 52/10 e seus Anexos;

b) Ata da Sessão Pública do Pregão Eletrônico n. 52/10;

c) Proposta da CONTRATADA, datada de ___/___/___.

Parágrafo segundo – A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões em até 25% (vinte e cinco por cento) do valor decorrente do presente Contrato, em razão de inclusão ou exclusão de componentes do objeto, sem modificação de preços e demais condições constantes de sua proposta, em conformidade com o parágrafo 1º do artigo 65 da LEI, correspondente ao parágrafo 1º do artigo 113 do REGULAMENTO, e previsto no subitem 1.2 do referido Edital.

Parágrafo terceiro – As supressões além desse limite são facultadas por acordo entre as partes, em conformidade com o artigo 65, §2º, inciso II, da LEI, correspondente ao artigo 113, §2º, do REGULAMENTO.

Parágrafo quarto - Os acréscimos e as exclusões de que trata este parágrafo somente serão permitidos até a entrega formal do documento contendo o Termo de Licença que dá direito à atualização da solução de segurança de estações de trabalho (*Endpoints*) oferecida.

CLÁUSULA SEGUNDA – DAS ESPECIFICAÇÕES TÉCNICAS

O objeto deste Contrato deverá obedecer rigorosamente às especificações técnicas descritas no Edital do Pregão Eletrônico n. 52/10, em especial no seu Anexo n. 2.

CLÁUSULA TERCEIRA – DA INSTALAÇÃO DA SOLUÇÃO

A instalação da solução objeto desta contratação será realizada conforme o Cronograma de Encadeamento de Fases constante do Anexo n. 4 ao Edital do Pregão Eletrônico n. 52/10.

Parágrafo primeiro – O cronograma referido no *caput* desta Cláusula destina-se a especificar ações de responsabilidade exclusiva da CONTRATADA e não incluem os dias despendidos pelo Centro de Informática nas análises e nas aferições necessárias à concessão dos aceites.

Parágrafo segundo – O prazo para início da fase 1 do Cronograma referido no *caput* desta Cláusula será contado a partir da data de assinatura deste Contrato.

Parágrafo terceiro – Os demais prazos de início serão contados a partir do aceite da fase anterior ou, no caso da fase 4, da data de envio da Ordem de Serviço, nos termos do item 2.4 do Anexo n. 4 ao Edital do Pregão Eletrônico n. 52/10.

Parágrafo quarto – Os prazos máximos de conclusão previstos no Cronograma deverão ser rigorosamente obedecidos, sob pena de aplicação de multa conforme previsto no Anexo n. 8 ao Edital do Pregão Eletrônico n. 52/10.

CLÁUSULA QUARTA – DA CAPACITAÇÃO OPERACIONAL

A capacitação operacional deverá habilitar servidores da CONTRATANTE na utilização plena da solução *Endpoint*, observadas as disposições contidas no Anexo n. 3 ao Edital do Pregão Eletrônico n. 52/10.

Parágrafo único – A capacitação operacional referida no *caput* desta Cláusula deverá ser concluída dentro do prazo previsto para o término da Fase 1 do Cronograma de Encadeamento das Fases, conforme descrito no Anexo n. 4 do referido Edital.

CLÁUSULA QUINTA – DA GARANTIA DE FUNCIONAMENTO, DA ATUALIZAÇÃO E DO SUPORTE TÉCNICO

O prazo do serviço de suporte técnico e garantia de funcionamento da solução será de, no mínimo, 24 (vinte e quatro) meses, para os subitens 1.1 a 1.5 do item único constante do Anexo n. 1 ao Edital do Pregão Eletrônico n. 52/10, contados da data do Recebimento Provisório da Solução (após a conclusão da Fase 3 do Cronograma de Encadeamento das Fases – Anexo n. 4 ao referido Edital).

Parágrafo primeiro – Para o subitem 1.9 do item único do Anexo n. 1 ao Edital do Pregão Eletrônico n. 52/10 o prazo de suporte técnico e garantia de funcionamento será de, no mínimo, 21 (vinte e um) meses, contados da data do Recebimento Definitivo da Solução (após a conclusão da Fase 4 constante do Cronograma de Encadeamento das Fases do Anexo n. 4 ao Edital do Pregão Eletrônico n. 52/10).

Parágrafo segundo **–** A prestação dos serviços de suporte técnico e garantia de funcionamento deverá obedecer rigorosamente às especificações descritas no Anexo n. 5 ao Edital do Pregão Eletrônico n. 52/10.

Parágrafo terceiro **–** A CONTRATADA fica obrigada a solucionar, sem custos, eventuais problemas relativos a defeitos ("*bugs*"), bem como a fornecer quaisquer correções ("*patches*") e atualizações disponibilizadas pelo fabricante da solução durante o período de garantia.

Parágrafo quarto - Para os efeitos da exigência do parágrafo anterior, entende-se como atualização, o provimento de toda e qualquer evolução, incluindo correções, "*updates*", "*service packs*", novas "*releases*", "*builds*" e funcionalidades, bem como o provimento de "*upgrades*" englobando, inclusive, versões não sucessivas e de novos produtos que substituam a solução em caso de descontinuidade, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado.

Parágrafo quinto – A CONTRATADA deverá entregar o produto na sua versão mais recente disponível comercialmente e executar os serviços associados descritos no Anexo n. 5 ao Edital do Pregão Eletrônico n. 52/10.

Parágrafo sexto **–** A CONTRATADA deverá formalmente informar e encaminhar ao Centro de Informática, no prazo máximo de 10 (dez) dias úteis após sua liberação ao mercado, as novas versões dos produtos contratados.

Parágrafo sétimo – O objeto contratual será recebido em quatro fases distintas, conforme Cronograma disposto no Título 3 do Anexo n. 4 ao Edital do Pregão Eletrônico n. 52/10, se em perfeitas condições e conforme as especificações editalícias a que se vincula a proposta da Contratada.

Parágrafo oitavo - O Recebimento Provisório da Solução se dará após a conclusão e o aceite da Fase 3 e o Recebimento Definitivo da Solução se dará após a conclusão e o aceite da Fase 4, **observado o disposto no Título 1 do Anexo n. 4** ao Edital do Pregão Eletrônico n. 52/10.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATADA

Constituem obrigações da CONTRATADA aquelas enunciadas no Edital do Pregão Eletrônico n. 52/10 e em seus anexos, além daquelas determinadas pelo órgão fiscalizador, em caráter complementar, visando à perfeita execução do objeto do presente Contrato.

Parágrafo primeiro – Todas as obrigações trabalhistas, inclusive aquelas relativas ao Fundo de Garantia por Tempo de Serviço (FGTS) e à Previdência Social, são de exclusiva responsabilidade da CONTRATADA, como única empregadora da mão-de-obra utilizada para os fins estabelecidos no presente Contrato.

Parágrafo segundo – A CONTRATADA responderá integral e exclusivamente por eventuais reclamações trabalhistas de seu pessoal, mesmo na hipótese de ser a UNIÃO (Câmara dos Deputados) acionada diretamente como Correclamada.

Parágrafo terceiro – A CONTRATADA fica obrigada a apresentar à CONTRATANTE, sempre que expire o prazo de validade, a Certidão Negativa de Débitos Relativos às Contribuições Previdenciárias e às de Terceiros (CND), a Certidão Conjunta Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União e o Certificado de Regularidade do FGTS (CRF).

Parágrafo quarto – A não apresentação das certidões e do certificado, na forma mencionada no parágrafo anterior, implicará o descumprimento de cláusula contratual, podendo, inclusive, ensejar a rescisão deste Contrato, nos termos do artigo 78 da LEI, correspondente ao artigo 126 do REGULAMENTO.

Parágrafo quinto - Os empregados da CONTRATADA, por esta alocados na execução dos serviços, embora sujeitos às normas disciplinares ou convencionais da CONTRATANTE, não terão com ela qualquer vínculo empregatício.

Parágrafo sexto - Todas as obrigações tributárias, trabalhistas e sociais da CONTRATADA e de seus empregados serão de inteira responsabilidade daquela.

Parágrafo sétimo - A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da CONTRATANTE ou de terceiros por ação ou omissão de seus empregados ou prepostos, na área de prestação dos serviços, mesmo que fora do exercício das atribuições previstas neste Contrato.

Parágrafo oitavo - A CONTRATADA comunicará, verbal e imediatamente, ao órgão fiscalizador, todas as ocorrências anormais verificadas na execução dos serviços e, em até 5 (cinco) dias após o ocorrido, reduzirá a escrito a comunicação verbal, acrescentando todos os dados e circunstâncias julgados necessários ao esclarecimento dos fatos.

Parágrafo nono - A CONTRATADA deverá reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto deste Contrato em que se verificarem imperfeições, vícios, defeitos ou incorreções resultantes da execução dos serviços ou de materiais empregados, por exigência do órgão fiscalizador, que lhe assinará prazo compatível com as providências ou reparos a realizar.

Parágrafo décimo – A CONTRATADA fica obrigada a manter durante toda a execução deste Contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas no momento da licitação.

Parágrafo décimo primeiro - A CONTRATADA deverá marcar, por meio do telefone (61) 3216-3793 ou email seseg.cenin@camara.gov.br, uma reunião preparatória que deverá ocorrer dentro do prazo de três dias, contados da data de assinatura do contrato, que tratará, dentre outros assuntos pertinentes, do cronograma de execução da capacitação operacional, do cronograma de implantação da solução e do modo de abertura de chamados técnicos.

CLÁUSULA SÉTIMA– DAS SANÇÕES ADMINISTRATIVAS

Pelo não cumprimento de suas obrigações contratuais, execução insatisfatória dos serviços, omissão ou outras faltas mencionadas no Título 12 do Edital do Pregão Eletrônico n. 52/10 e em seu Anexo n. 8, serão aplicadas à CONTRATADA as multas e demais sanções previstas nos respectivos dispositivos, observadas as condições neles indicadas.

CLÁUSULA OITAVA – DO PREÇO E DO PAGAMENTO

O preço total do presente Contrato é de R$ (valor numérico e por extenso), considerando-se os preços unitários constantes da proposta da CONTRATADA.

Parágrafo primeiro – O pagamento dos **subitens 1.1 a 1.7, 1.9 e 1.10** do Título 1 do Anexo n. 1 ao Edital de Pregão Eletrônico n. 52/10, referentes à entrega dos componentes, realização da capacitação operacional, configuração e ativação da solução, distribuição das funcionalidades configuradas nos equipamentos em rede para a Câmara dos Deputados e por esta aceitos, será feito de acordo com o Cronograma de Encadeamento das Fases disposto no Título 3 do Anexo n. 4, por meio de depósito em conta corrente da CONTRATADA, em agência bancária indicada, mediante a apresentação, em duas vias, de nota fiscal/fatura discriminada, após emissão do Aceite Provisório ou Definitivo, conforme o caso, pelo órgão fiscalizador.

Parágrafo segundo -O pagamento dos serviços referentes à garantia de funcionamento (suporte técnico) e atualização da solução se dará conforme abaixo:

a) Os serviços de suporte técnico e de Atualização da Solução por um período de 24 meses (**subitem 1.8** do Título 1 do Anexo n. 1 ao Edital de Pregão Eletrônico n. 52/10) executados pela CONTRATADA e aceitos pela CONTRATANTE será efetuado em vinte e quatro parcelas mensais, após o primeiro mês de prestação dos referidos serviços, que terão início a partir da data do Recebimento Provisório da Solução – (após a conclusão da Fase 3 do Cronograma de Encadeamento das Fases), não se admitindo o pagamento antecipado sob qualquer pretexto.

b) Os serviços referentes ao Suporte Técnico e de Atualização por um período de 21 meses para 5.900 licenças de uso da funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (**subitem 1.11** do Título 1 do Anexo n. 1 ao Edital do Pregão Eletrônico n. 52/10) executados pela contratada e aceitos definitivamente pela Câmara dos Deputados será efetuado em vinte e uma parcelas mensais, após o primeiro mês de prestação dos referidos serviços, que terão início a partir da data do Recebimento Definitivo da Solução (após a conclusão da Fase 4 do Cronograma de Encadeamento das Fases), não se admitindo o pagamento antecipado sob qualquer pretexto.

Parágrafo terceiro – O pagamento de cada parcela será efetuado por meio de depósito em conta corrente da CONTRATADA, em agência bancária indicada, mediante a apresentação em duas vias de nota fiscal/fatura discriminada, emitida no mês subsequente ao da prestação dos serviços, após atestação pelo órgão fiscalizador.

Parágrafo quarto – A instituição bancária, a agência e o número da conta deverão ser mencionados na nota fiscal/fatura.

Parágrafo quinto – A nota fiscal/fatura deverá vir acompanhada da Certidão Negativa de Débitos Relativos às Contribuições Previdenciárias e às de Terceiros (CND) e do Certificado de Regularidade do FGTS – CRF, ambos dentro dos prazos de validade neles expressos.

Parágrafo sexto – O pagamento será feito com prazo não superior a 30 (trinta) dias, contados a partir do aceite dos serviços e da comprovação da regularidade da documentação fiscal apresentada, prevalecendo a data que ocorrer por último.

Parágrafo sétimo - Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pela CONTRATANTE, entre a data referida no parágrafo anterior e a correspondente ao efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, são calculados por meio da aplicação da fórmula constante do subitem 13.5.1 do Edital do Pregão Eletrônico n. 52/10.

Parágrafo oitavo – Quando aplicável, o pagamento efetuado pela CONTRATANTE estará sujeito às retenções de que trata o artigo 31 da Lei n. 8.212, de 1991, com a redação dada pelas Leis n. 9.711, de 1998, e n. 11.933, de 2009, além das previstas no artigo 64 da Lei n. 9.430, de 1996, e demais dispositivos legais que obriguem a retenção de tributos.

Parágrafo nono – Estando a CONTRATADA isenta das retenções referidas no parágrafo anterior, a comprovação deverá ser anexada à respectiva fatura.

CLÁUSULA NONA – DA CLASSIFICAÇÃO ORÇAMENTÁRIA

A despesa com a execução do presente Contrato, objeto da Nota de Empenho n. 2010NE_____, correrá à conta da seguinte classificação orçamentária:

Programas de Trabalho:

01.031.0553.4061.0001 – Processo Legislativo e

01.128.0553.4091.0001 – Capacitação de Recursos Humanos

Naturezas da Despesa
3.0.00.00 - DESPESAS CORRENTES
3.3.00.00 - OUTRAS DESPESAS CORRENTES
3.3.90.00 - APLICAÇÕES DIRETAS
3.3.90.39 - Outros Serviços de Terceiros (Pessoa Jurídica)
e
4.0.00.00 - DESPESAS DE CAPITAL
4.4.00.00 - INVESTIMENTOS
4.4.90.00 - APLICAÇÕES DIRETAS
4.4.90.39 - Outros Serviços de Terceiros (Pessoa Jurídica)

CLÁUSULA DÉCIMA – DA VIGÊNCIA E DA RESCISÃO

O presente Contrato terá vigência de ___/___/___ a ___/___/___, ou seja, até o término do prazo de garantia de funcionamento e atualização da solução.

Parágrafo primeiro - Este Contrato poderá ser prorrogado para prestação de serviços de suporte técnico e atualização, em conformidade com o inciso II do Artigo 57 da LEI, e com o inciso II do Artigo 105 do REGULAMENTO, a critério da CONTRATANTE.

Parágrafo segundo – Este Contrato poderá ser rescindido nos termos das disposições contidas nos artigos 77 a 80 da LEI, correspondentes aos artigos 125 a 128 do REGULAMENTO.

CLÁUSULA DÉCIMA PRIMEIRA – DA REPACTUAÇÃO DO PREÇO

O preço global mensal contratado referente aos serviços de garantia de funcionamento e atualização poderá ser repactuado, desde que observado interregno mínimo de 1 (um) ano, a contar da data da proposta, ou da data do orçamento a que a proposta se referir, ou da data da última repactuação, cabendo à CONTRATADA, na oportunidade de sua solicitação, justificar e comprovar a variação dos componentes dos custos do Contrato, apresentando, inclusive, Memória de Cálculo e Planilhas apropriadas para análise e posterior aprovação da CONTRATANTE.

CLÁUSULA DÉCIMA SEGUNDA– DO ÓRGÃO FISCALIZADOR

Considera-se órgão fiscalizador do presente Contrato o Centro de Informática - CENIN da Câmara dos Deputados, situado no 11º andar do Edifício Anexo I, que designará servidor responsável pelos atos de acompanhamento e fiscalização desta contratação.

CLÁUSULA DÉCIMA TERCEIRA – DO FORO

Fica eleito o foro da Justiça Federal em Brasília, Distrito Federal, com exclusão de qualquer outro, para decidir as demandas judiciais decorrentes do cumprimento deste Contrato.

E por estarem assim de acordo, as partes assinam o presente instrumento em três vias de igual teor e forma, para um só efeito, com ___ (valor numérico e por extenso) folhas cada, na presença das testemunhas abaixo indicadas.

Brasília, de de 2010.

Pela CONTRATANTE:	Pela CONTRATADA:
Sérgio Sampaio C. de Almeida	(nome)
Diretor-Geral	(cargo)
CPF n. 358.677.601-20	(CPF)

Testemunhas: 1) _____

2) _____\

Brasília, 11 de março de 2010.

José Martinichen Filho
Pregoeiro