PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CONTRATO N. 047/2011 – CJF

PROCESSO N. 2011161305

PREGÃO ELETRÔNICO N. 46/2011

DADOS SOBRE A EMPRESA
CONTRATADA: Fast Security Tecnologia da Informação Ltda.
CNPJ/MF: 10.647.012/0001-66
ENDEREÇO: SCIA, Quadra 14, Conjunto 3, Lote 3, 1º andar, Parte A, Guará, Brasília-DF
CEP: 71.250-115
TELEFONE/E-MAIL: (61) 3363-8636/ comercial@fasthelp.inf.br
REPRESENTANTE: Gustavo Lima Miranda

DADOS DO CONTRATO
OBJETO: contratação de uma solução de antivírus
FUNDAMENTAÇÃO LEGAL: Lei n. 10.520, de 17 de julho de 2002, no Decreto n. 5.450/2005, Resolução n. 98 de 10 de novembro de 2009 do Conselho Nacional de Justiça, Lei Complementar n. 123/2006 e subsidiariamente na Lei n. 8.666, de 21 de junho de 1993 e suas alterações, no Processo n. 2011161305
VIGÊNCIA: 04 meses, contados da assinatura
GARANTIA: 48 meses, contados do recebimento definitivo
VALOR DO CONTRATO: R$ 95.883,00
UNIDADE FISCALIZADORA: STI – Seção de Suporte à Infraestrutura

Antonio Humberto Machado de Sousa Brito
Secretário-Geral

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CONTRATO N. 047/2011-CJF

CONTRATO DE FORNECIMENTO DE SOLUÇÃO ANTIVÍRUS QUE ENTRE SI CELEBRAM O CONSELHO DA JUSTIÇA FEDERAL E A EMPRESA FAST SECURITY TECNOLOGIA DA INFORMAÇÃO LTDA.

A **UNIÃO,** por intermédio do **CONSELHO DA JUSTIÇA FEDERAL**, Órgão integrante do Poder Judiciário, inscrito no CNPJ/MF sob o n. 00.508.903/0001-88, com sede no SCES, Trecho 03, Lote 09, Polo 08, Brasília-DF, doravante denominado CONTRATANTE, neste ato representado por sua Secretária-Geral, Senhora EVA MARIA FERREIRA BARROS, brasileira, solteira, inscrita no CPF/MF n. 188.490.083-68 e portadora da C.I. n. 666.351 SSP/DF, residente e domiciliada nesta Capital, e a empresa **FAST SECURITY TECNOLOGIA DA INFORMAÇÃO LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o n. 10.647.012/0001-66, com sede no SCIA, Quadra 14, Conjunto 3, Lote 3, 1º andar, Parte A, Guará, Brasília-DF, doravante denominada CONTRATADA, neste ato representada por seu Diretor de Operações, Senhor GUSTAVO LIMA MIRANDA, brasileiro, inscrito no CPF/MF sob o n. 707.868.101-06 e portador da C.I. nº 1.828.256 SSP-DF, residente e domiciliado nesta Capital, CELEBRAM, com fundamento na Lei n. 10.520, de 17 de julho de 2002, no Decreto n. 5.450/2005, Resolução n. 98 de 10 de novembro de 2009 do Conselho Nacional de Justiça, Lei Complementar n. 123/2006 e subsidiariamente na Lei n. 8.666, de 21 de junho de 1993 e suas alterações, no Processo n. 2011161305, o presente **CONTRATO DE FORNECIMENTO E PRESTAÇÃO DE SERVIÇOS** mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 – O presente contrato tem por objeto a contratação de uma solução de antivírus, em estrita conformidade com as características técnicas obrigatórias estabelecidas neste Contrato e seu MÓDULO: I – Termo de Referências e seus anexos, compreendendo os serviços de:

a) Instalação e configuração;

b) Garantia pelo período de 48 (quarenta e oito meses);

c) Transferência de conhecimento para 02 participantes, com no mínimo 16 (dezesseis) horas;

d) Suporte Técnico, durante o período de garantia

1.1.1 – Composição da solução:

1.1.1.1 Renovação e complementação das licenças de antivírus TREND MICRO atualmente instaladas no CJF, (subitem 3.1, Anexo I termo de referência); ou

1.1.1.2 Substituição da solução de antivírus atualmente implantada nas instalações do Contratante.

1.2 - Independentemente das opções descritas acima, as soluções devem possuir licenciamento para a completa proteção do ambiente tecnológico descrito do subitem 3.2, Módulo I-Termo de Referência.

1.3. O detalhamento do objeto é apresentado no Módulo I -Termo de Referência e seus anexos, o qual adere a este contrato e dele faz parte, independentemente de transcrição.

CLÁUSULA SEGUNDA – DOS SERVIÇOS

A entrega e instalação das licenças deverão ser nas dependências do Contratante, a saber, edifício sede localizado SCES TRECHO III, PÓLO 08, LOTE 09 e Coordenadoria Gráfica localizada no SAAN Quadra 01, Lotes 10/70.

2.1. A CONTRATADA deverá iniciar a execução deste contrato após sua assinatura, conforme Cronograma de Implantação - Anexo III do Módulo I.

2.1.1. No dia seguinte à assinatura deste contrato, será realizada reunião no CONTRATANTE em sua SEDE com o objetivo de planejar e coordenar as atividades de fornecimento, instalação, configuração e testes dos produtos.

2.1.2. Após a reunião no item acima, a CONTRATADA apresentará um Plano Executivo, no prazo de 5 (cinco) dias da assinatura do contrato, contendo a documentação detalhada de todo o planejamento para instalação dos produtos.

2.1.3. O Plano Executivo deverá dispor sobre o cronograma de implantação da solução contratada, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pelo CONTRATANTE e CONTRATADA e indicar os principais riscos e forma de mitigação, contendo no mínimo os seguintes itens:

a) Conferência das licenças entregues;
b) Pré-instalação (se for o caso);
c) Pré-testes;
d) Instalação e configuração;
e) Teste de operação;
f) Ativação da solução;
g) Entrega da documentação atualizada dos produtos; e
h) Treinamento / Transferência de conhecimento.

2.2. Os técnicos da CONTRATADA que prestarão os serviços de instalação/ migração deverão ser certificados pelo fabricante nos produtos que compõem a solução de antivírus, devendo ser apresentada a correspondente documentação de certificação em versão original ou cópia autenticada.

2.3. A Contratada deverá indicar responsável técnico pelo projeto proposto (gerente de projeto), com certificação PMP (Project Management Professional) ou com experiência comprovada em gerenciamento de projetos.

2.4. Os softwares deverão ser entregues em até 15 (quinze) dias da assinatura deste contrato.

2.4.1. Juntamente com o software, deverá ser entregue toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização e os demais documentos indicados no item **3.7.8** do Módulo I e seu Anexo II.

2.5. O serviço de instalação, atualização ou migração, configuração da solução e transferência de conhecimento deverá ser concluído no prazo de 15 (quinze) dias corridos, contados a partir do Recebimento Provisório.

2.6. Os Procedimentos para implantação da solução são os constantes do item 4.2 do Módulo I deste Contrato.

CLÁUSULA TERCEIRA – DO TREINAMENTO/TRANSFERÊNCIA DE CONHECIMENTO

3.1 – A CONTRATADA deverá prestar os serviços de treinamento oficial do fabricante para 02 (dois) participantes, com carga horária mínima de 16 horas, contemplando a perfeita instalação, operação, manuseio, gerenciamento, configuração e utilização dos produtos descritos no Módulo I – Termo de Referência deste Contrato.

3.2 - O treinamento deverá ser realizado em Brasília-DF e a CONTRATADA deverá providenciar as instalações para o treinamento.

3.3. O programa para treinamento/ atualização de conhecimento tecnológico deverá ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdos solicitadas deverão constar do material didático;

3.4. Deverá ser disponibilizado material didático impresso e em mídia, sem custo adicional para o CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês);

3.5. Deverá ser emitido certificado de participação ao final do curso a cada participante.

3.6. O cronograma efetivo do treinamento será definido em conjunto com o CONTRATANTE, após a assinatura do contrato;

3.6.1. Para todos os efeitos, inclusive de emissão do Termo de Recebimento Definitivo, o treinamento faz parte do processo de implantação da solução;

3.6.2. Caso o treinamento/ atualização fornecido não for satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizá-los novamente, sem ônus adicional ao CONTRATANTE.

3.6.3. Este treinamento deverá ser realizado por técnico qualificado e certificado pelo fabricante da solução fornecida.

CLÁUSULA QUARTA – DA GARANTIA E SUPORTE TÉCNICO

4.1 - O prazo de garantia dos produtos é de, no mínimo, 48 (quarenta e oito) meses, contados a partir da data do recebimento definitivo.

4.2. A solução terá prazo de garantia de funcionamento e de direito a atualização de versões durante a vigência deste contrato.

4.2.1. No valor do software já deve estar incluso os custos da garantia.

4.3. Durante o prazo de garantia, a contratada deverá providenciar, sem ônus adicional para o Contratante, o fornecimento de atualização de versão e/ou release, bem como patches de todos os softwares que integram a solução, incluindo drivers e todos os demais elementos integrantes da solução fornecida.

4.4. A garantia consiste, entre outros:

4.4.1. Na reparação das eventuais falhas de funcionamento, mediante a substituição de versão, de acordo com os manuais e normas técnicas específicas.

4.4.2. Na orientação das melhores práticas de uso do produto adquirido.

4.4.3. Todas as atualizações, novas versões e releases do software.

4.5. A CONTRATADA deverá disponibilizar a atualização dos produtos licenciados assim que houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;

4.5.1. O direito de atualização de versão de cada programa deverá abranger:

4.5.1.1. Logo após a contratação e sempre que for lançada nova versão ou release de qualquer programa integrante do conjunto de programas, a Contratada deverá enviar ao Contratante, em até 15 dias úteis, um conjunto de mídias de instalação da versão fornecida ou atualizada e nota informativa das funcionalidades implementadas na nova versão. Será aceita a disponibilização das atualizações no sítio do fabricante, como alternativa ao envio das mídias;

4.5.1.2. Download de drivers, firmwares, patches, atualizações dos programas e manuais técnicos, a partir do sítio internet do fabricante do produto;

4.5.1.3. Todas as atualizações, novas versões e releases dos programas que fizerem parte da solução contratada;

4.5.1.4. Direito de acesso pelos técnicos do Contratante à base de conhecimento e a fóruns da solução no sítio do fabricante;

4.5.1.5. A contratada deverá notificar o Contratante em prazo não superior a 10 (dez) dias sobre a disponibilidade de novas versões e releases dos softwares que fizerem parte da solução fornecida;

4.5.2. Juntamente com a documentação de instalação da solução, como requisito para o aceite definitivo da solução, a contratada deverá entregar a seguinte documentação:

4.5.2.1. Certificados de garantia de que todos os produtos estão cobertos pela garantia, por todo o período contratado, incluindo as extensões de garantia do fabricante, de forma que sejam atingidos os 48 (quarenta e oito) meses totais exigidos.

4.5.2.2. Caso não seja comercializada extensão de garantia com o prazo ou nos moldes exigidos no item anterior, deverá ser entregue pela contratada uma declaração nesse sentido, fornecida pelo fabricante dos equipamentos ou seu representante legal no Brasil. Nesse caso, a contratada assumirá a resolução dos defeitos eventualmente apresentados pelo software por seus próprios meios durante o período complementar à garantia original, até término do contrato;

4.5.2.3. Cessões de direito de uso perpétuo dos programas fornecidos. Os termos de licenciamento de todos os programas fornecidos, emitidos pelo fabricante, deverão ser entregues pela contratada e os mesmos serão direito pertencentes ao Conselho;

4.5.2.4. Conjunto de direitos de atualização de versão, pelo período de 48 meses de garantia, de todos os programas fornecidos. Abrangerá todos os programas e licenças a serem fornecidos. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela contratada e comporão direito pertencente ao patrimônio do Conselho.

4.6. A CONTRATADA deverá disponibilizar suporte técnico de toda a solução, através da forma de atendimento remoto, em período integral – 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, pelo período de garantia da solução.

4.7. O CONTRATANTE fará a "abertura de chamados" técnicos

através de ligação telefônica ou via web, em período integral 24 (vinte e quatro) horas por dia 07 (sete) dias por semana. A CONTRATADA deverá informar o número do telefone em sua proposta. Se a Central de Suporte estiver localizada fora de Brasília, a Contratada deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

4.8. A CONTRATADA deverá Realizar atendimentos "on-site" (Severidade 1 e 2) e remotos (Severidade 3 e 4) conforme categorização definida.

4.8.1. O atendimento deverá ser categorizado em quatro níveis. A contratada deverá garantir tempo máximo de atendimento e restauração de serviço, conforme tabela abaixo:

Criticidade	**Descrição**	**Prazo máximo de atendimento**	**Prazo máximo para restauração de serviço**
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto na operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 1 (uma) hora deve ter um técnico do fornecedor On-site.	Em até 6 horas
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 2 horas deve ter um técnico do fornecedor On-site.	Em até 10 horas
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Em até 4 horas um técnico do fornecedor entra em contato.	Em até 24 horas

Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 72 horas

4.8.2. Na abertura do chamado, a Contratada deverá informar o número da ordem de serviço;

4.8.3. A Contratada deverá enviar mensalmente um relatório consolidado das ordens de serviço geradas no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, os problemas verificados, as recomendações e orientações técnicas;

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

4.8.5. A Contratada deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CJF, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações;

4.8.6. A Contratada deverá orientar o CONTRATANTE para, quando for conveniente à CONTRATANTE, proceder à aplicação de pacotes de correção e implantação de versões do produto, cabendo à CONTRATADA orientar e disponibilizar um técnico para contato, em caso de dúvidas ou falhas, por meio telefônico ou correio eletrônico;

4.8.7. A Contratada deverá promover o isolamento, identificação e caracterização de falhas de laboratório (bugs), encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução.

4.8.7.1. Serão consideradas falhas de laboratórios o comportamento ou características dos programas que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados pela CONTRATANTE como prejudiciais ao seu uso.

CLÁUSULA QUINTA - DA RELAÇÃO EMPREGATÍCIA E DOS ENCARGOS SOCIAIS

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

CLÁUSULA SEXTA - DAS OBRIGAÇÕES E RESPONSABILIDADES DAS PARTES

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

a) responder por todas as despesas decorrentes do fornecimento/serviços objeto deste contrato;

b) manter, durante todo o período de vigência do ajuste, todas as condições que ensejaram sua contratação, particularmente no que tange à regularidade fiscal e à capacidade técnica e operativa;

c) prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CJF, em relação à instalação, configuração, migração e problemas detectados, atendendo de imediato as solicitações;

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

e) respeitar o sistema de segurança do CONTRATANTE, apresentando aos gestores do Contrato a relação dos empregados autorizados a prestar serviços de suporte técnico, devendo promover, de imediato, a substituição daqueles que, a critério do Contratante, venham a demonstrar conduta nociva ou incapacidade técnica;

f) realizar o treinamento/transferência de conhecimento;

g) deverá obter todas as licenças, autorizações e franquias necessárias à execução dos serviços de suporte técnico, pagando os emolumentos prescritos em lei;

h) aceitar, nas mesmas condições contratuais, as alterações e supressões que se fizerem necessárias, nos termos do art. 65 da Lei nº 8.666/93;

i) arcar com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a serem devidos em decorrência da execução dos fornecimentos/serviços de suporte técnico;

j) responsabilizar-se, pelos ônus resultante de quaisquer ações judiciais que venham a ser atribuídas ao CJF, relacionados com o cumprimento das obrigações assumidas no presente Contrato;

k) prestar os serviços de garantia e suporte técnico nas dependências do Contratante, no edifício Sede e Gráfica;

l) demais obrigações constantes do item 4 do Módulo I deste Contrato.

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

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

a) fornecer todas as informações e esclarecimentos solicitados pela Contratada;

b) acompanhar e fiscalizar a execução das obrigações deste Contrato;

c) efetuar os pagamentos com observância do prazo fixado.

d) demais obrigações constantes do item 5 do Módulo I – Termo de Referência, anexo deste Contrato.

CLÁUSULA SÉTIMA - DOS PREÇOS

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

7.2 - Os preços firmados neste contrato para os itens 1, 3 e 4 constante da Planilha de Preços são fixos e irreajustáveis.

7.3. O reajuste do suporte técnico, item 2 da planilha de preços, será efetuado conforme Cláusula 10 deste contrato.

CLÁUSULA OITAVA – DO RECEBIMENTO E DO PAGAMENTO

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

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

8.2.1 - provisoriamente, no prazo máximo de 30 (trinta) dias corridos a partir da entrega dos softwares, Plano Executivo e demais documentações da solução, conforme descrito no cronograma do Anexo III. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE, mediante Termo de Recebimento Provisório, assinado pelas partes;

8.2.2 - definitivamente, no prazo máximo de 30 (trinta) dias corridos, após a formalização por escrito da Contratada referente a conclusão de todas as fases de implantação da solução e desde que a CONTRATADA atenda a todas as solicitações da Comissão de Recebimento e Fiscalização do CONTRATANTE mediante Termo de Recebimento Definitivo, assinado pelas partes e desde que a CONTRATADA.

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

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

a.1) na hipótese de substituição a Contratada deverá providenciar sem que isso implique acréscimo aos preços contratados, a substituição de qualquer software, componente ou periférico por outro novo, de primeiro uso, com características idênticas ou superiores, no prazo de 72 (setenta e duas) horas, independente do fato de ser ou não fabricante da solução fornecidas, nos seguintes casos:

a.1.1.) se apresentar divergência com as especificações descritas na proposta apresentada;

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

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

8.4 – O pagamento será efetuado somente após o RECEBIMENTO DEFINITIVO. Este caracterizar-se-á pela emissão/juntada de Termo de Recebimento Definitivo emitido na forma do item 8.2 e aposição de Atesto no verso da Nota Fiscal de cobrança que ficará a cargo da Secretaria de Tecnologia da Informação do CONTRATANTE, no caso da Solução.

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

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

8.4.1 Nenhum pagamento será efetuado enquanto pendente o cumprimento de qualquer obrigação imposta à CONTRATADA inclusive em virtude de penalidade ou inadimplência.

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

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

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

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

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

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

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

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

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

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

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

8.15. Poderá o CONTRATANTE, após efetuar análise das notas fiscais de cobrança, efetuar descontos sobre os valores cobrados.

8.15.1. Ocorrendo descontos, este será deduzido da própria nota fiscal de cobrança, devendo o CONTRATANTE oficiar à CONTRATADA sobre as razões que o ensejaram.

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

CLÁUSULA NONA – DA VIGÊNCIA

9.1 – A vigência deste Contrato será de 04 (quatro) meses contados da data de assinatura, destinado a entrega da documentação, instalação da solução e transferência de conhecimento.

9.2 – O prazo de garantia com suporte técnico será 48 (quarenta e oito) meses, contados da data do recebimento definitivo.

CLÁUSULA DÉCIMA - DO REAJUSTE

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

10.2 Nos termos do acórdão do Tribunal de Contas da União, o reajuste deverá ser solicitado antes da prorrogação do contrato sob pena de a CONTRATADA incorrer em preclusão lógica.

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

11.1. O valor do presente contrato é de R$ 95.883,00 (noventa e cinco mil oitocentos e oitenta e três reais).

11.2. As despesas com a execução deste contrato serão atendidas, no exercício de 2011, com os recursos consignados no Orçamento Geral da União e suplementações a ele incorporadas, no Programa de Trabalho 000.821 e Elemento de Despesa 33.90.39.

11.3. Foi emitida a Nota de Empenho n.º 2011NE000753, no valor de R$ 95.883,00 (noventa e cinco mil oitocentos e oitenta e três reais) à conta da dotação orçamentária especificada no item 11.2 deste contrato.

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

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

12.1. Para os fins previstos no art. 86 da Lei 8.666/93, fica estipulados os percentuais mencionados a seguir, a título de multa de mora por dia em caso de atraso injustificado de 0,5% (cinco décimos por cento) sobre o valor total da contratação até o limite de 10% (dez por cento) do valor contratado. Após 15(quinze) dias úteis de atraso

no fornecimento da solução de segurança, o CJF poderá considerar como inexecução parcial do objeto.

12.2. Multa de 5% (cinco por cento) sobre o valor mensal para o serviço de Suporte Técnico, por hora de atraso no caso do descumprimento dos prazos de atendimento, limitado a 30% (trinta por cento) sobre o valor do contrato.

12.3. Em caso de inexecução total ou parcial do objeto deste Contrato, em razão do descumprimento de qualquer das condições avençadas, a Contratada ficará sujeita às seguintes penalidades, a critério da Administração, nos termos do art. 87 da Lei 8.666/93: I - advertência; II - multa de 10% (dez por cento) da obrigação inadimplida: III - suspensão temporária de participação em licitação e impedimento de contratar com a Administração por 02 (dois) anos e IV - declaração de inidoneidade para licitar ou contratar com a Administração Pública.

12.4. As sanções previstas nos incisos I, III e IV do art. 87 da Lei 8.666/93 poderão ser aplicadas juntamente com a do inciso II do mesmo artigo.

12.5. O valor da multa aplicada, após regular processo administrativo, será descontado dos pagamentos devidos pela Administração ou cobrado judicialmente a critério da Administração.

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

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

CLÁUSULA DÉCIMA TERCEIRA - DA RESCISÃO

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

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

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

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

CLÁUSULA DÉCIMA QUARTA - DA LICITAÇÃO

14.1. A presente contratação foi antecedida de procedimento licitatório na modalidade Pregão Eletrônico nº 46/2011, razão pela qual ficam fazendo parte integrante do ajuste, independentemente de transcrição, as disposições contidas no instrumento convocatório, bem como as condições propostas pela CONTRATADA naquilo em que não contrariarem o que aqui ficou estipulado.

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

CLÁUSULA DÉCIMA QUINTA - DA FISCALIZAÇÃO

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

15.2. Caberá a Seção de Suporte à Infraestrutura do CONTRATANTE exercer a fiscalização acima estabelecida.

15.2.1. Será designado pela autoridade competente da administração, um Fiscal Administrativo encarregado da fiscalização do contrato quanto aos aspectos administrativos.

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

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

CLÁUSULA DÉCIMA SEXTA - DA PUBLICAÇÃO

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

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

CLÁUSULA DÉCIMA SÉTIMA - DO FORO

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

CLÁUSULA DÉCIMA OITAVA - DAS DISPOSIÇÕES FINAIS

18.2 - No prazo de até 05 (cinco) dias úteis após a assinatura deste contrato, a CONTRATADA credenciará junto ao CONTRATANTE preposto apto a representá-la durante a execução deste contrato.

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

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

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

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

Brasília-DF, 30 de dezembro de 2011.

Antonio Humberto Machado de Sousa Brito
Secretário-Geral, em exercício

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

GUSTAVO LIMA MIRANDA
Diretor de Operações da empresa
Fast Security Tecnologia da Informação Ltda

ANEXO AO CONTRATO N. 047/2011 – CJF

MÓDULO I
PREGÃO ELETRÔNICO N.º 46/2011-CJF
PROCESSO 2011161305

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Contratação de solução de antivírus com garantia de 48 meses, contemplando serviços de instalação e configuração, transferência de conhecimento e suporte técnico, podendo ser composta conforme os seguintes subitens:
1.1.2. Renovação e complementação das licenças de antivírus TREND MICRO atualmente instaladas no CONTRATANTE (subitem 3.1); ou
1.1.3. Substituição da solução de antivírus atualmente implantada no CONTRATANTE.
1.2. Independentemente das opções descritas acima, as soluções devem possuir licenciamento para a completa proteção do ambiente tecnológico descrito no subitem 3.2.

2. (...)

3. DESCRIÇÃO DOS PRODUTOS

3.1. QUADRO DEMONSTRATIVO DA SITUAÇÃO ATUAL DE LICENÇAS – SOLUÇÃO TREND MICRO

PRODUTO	QUANTIDADE DE LICENÇAS
Control Manager Advanced - Component	391
Email Reputation Services	450
Imss – V 7.0 Standard Linux - Of	450
Officescan Superkey (AV+SW+DC+FW) English	391
Serverprotect Linux Component	391
Serverprotect Multiplataforma 5x - Of	391
Spam Prevention Solution – Only V 7.0 – Linux Of	450

3.2. AMBIENTE TECNOLÓGICO DO CJF PARA DIMENSIONAMENTO DA COMPLEMENTAÇÃO DE LICENÇAS DA ATUAL SOLUÇÃO OU FORNECIMENTO DE LICENÇAS DE OUTROS FABRICANTES

PRODUTO	QUANTIDADE
Estações de trabalho - Windows	450
Servidores Windows	30
Servidores Linux	90
Armazenamento Centralizado de Dados - Storage	02
Servidor de correio eletrônico	01
Gerência da solução de antivírus	01

3.2.1. A LICITANTE deverá escolher o tipo de licenciamento que melhor atenda a sua política comercial para proteção do ambiente descrito acima;
3.3. O detalhamento do ambiente tecnológico do CJF está descrito no ANEXO II.

OBRIGAÇÕES DA CONTRATADA

3.4. Quanto aos serviços

A Contratada deverá:
3.4.1. Iniciar a execução do contrato após sua assinatura.
3.4.2. No dia seguinte à assinatura do contrato, deverá ser realizada reunião no CONTRATANTE SEDE com o objetivo de planejar e coordenar as atividades de fornecimento, instalação, configuração e testes dos produtos. Com base nesta reunião, a CONTRATADA deverá apresentar um Plano Executivo, em até 5

(cinco) dias da assinatura do contrato, contendo a documentação detalhada de todo o planejamento para instalação dos produtos. O Plano Executivo deverá dispor sobre o cronograma de implantação da solução contratada, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pelo CONTRATANTE e CONTRATADA e indicar os principais riscos e forma de mitigação, contendo no mínimo os seguintes itens:

a) Conferência das licenças entregues;
b) Pré-instalação (se for o caso);
c) Pré-testes;
d) Instalação e configuração;
e) Teste de operação;
f) Ativação da solução;
g) Entrega da documentação atualizada dos produtos; e
h) Treinamento / Transferência de conhecimento.

3.4.3. Os técnicos da CONTRATADA que prestarão os serviços de instalação/ migração deverão ser certificados pelo fabricante nos produtos que compõem a solução de antivírus, devendo ser apresentada a correspondente documentação de certificação em versão original ou cópia autenticada.

3.4.4. Indicar responsável técnico pelo projeto proposto (gerente de projeto), com certificação PMP (Project Management Professional) ou com experiência comprovada em gerenciamento de projetos.

3.4.5. Entregar os softwares em até 15 (quinze) dias da assinatura do contrato.

3.4.6. Entregar, juntamente com o software, toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização e o demais documentos indicados no item 3.7.8 e Anexo II.

3.4.7. Receber cópia do "Termo de Recebimento Provisório", após entrega dos softwares, Plano Executivo e demais documentações da solução, conforme descrito no cronograma do Anexo III. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação formal de entrega, desde que não haja pendências a cargo da CONTRATADA.

3.4.8. Concluir no prazo de 15 (quinze) dias corridos, contados a partir do Termo de Recebimento Provisório, o serviço de instalação, atualização ou migração, configuração da solução e transferência de conhecimento.

3.4.9. Receber cópia do "Termo de Recebimento Definitivo", que deverá ser providenciado pela CONTRATANTE no prazo máximo de 15 (quinze) dias corridos, após a formalização por escrito da Contratada referente a conclusão de todas as fases de implantação da solução e desde que a CONTRATADA atenda a todas as solicitações da Comissão de Recebimento e Fiscalização da CONTRATANTE.

3.5. Procedimentos para implantação da solução

3.5.1. Caso a solução a ser fornecida, seja diferente do software de antivírus atualmente instalado no CJF, a contratada deverá providenciar a desinstalação automática de todas as cópias instaladas do software em estações e servidores, e a instalação do novo software de antivírus em um único processo.

3.5.2. Esta instalação deve ser feita por técnico qualificado e certificado pelo fabricante da solução ofertada.

3.5.3. Caso a solução seja a mesma já existente, a mesma deve ser atualizada para última versão disponível e toda a configuração revisada e correções ou melhorias deverão ser implementadas.

3.5.4. A CONTRATADA será inteiramente responsável pela instalação, atualização ou migração da solução antivírus atualmente em uso pelo CONTRATANTE, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica.

3.5.5. A instalação, atualização ou migração dos softwares em estações de trabalho deverá ser realizada remotamente, sem causar indisponibilidade de cada estação superior a 10 (dez) minutos, devendo ser realizada em horários a serem definidos pelo CONTRATANTE.

3.5.6. A instalação, atualização ou migração dos softwares em servidores de rede deverá ser realizada remotamente, ou localmente a critério do CONTRATANTE, devendo ser realizada em horários que não coincidam com o expediente da CONTRATANTE, preferencialmente, sem causar indisponibilidade nos servidores e serviços em produção.

3.5.7. O CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção.

3.5.8. O processo de instalação, atualização ou migração da solução deverá ser acompanhado por analistas do CONTRATANTE.

3.5.9. Para garantir que a instalação, atualização ou migração não afetará o ambiente do

CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante, nos produtos envolvidos, comprovado no ato de entrega do Plano Executivo.

3.5.10. A CONTRATADA estará vinculada ao estrito cumprimento do ANEXO III – Cronograma de Implantação.

3.5.11. A Contratada deverá garantir sigilo e inviolabilidade das informações que eventualmente possa ter acesso durante os procedimentos de instalação.

3.5.12. A Contratada deverá ser responsável pelo pagamento das despesas de custeio do deslocamento do(s) seu(s) técnico(s) às dependências do CJF, bem como por todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos na prestação dos serviços contratados.

3.5.13. A Contratada deverá arcar com todos os encargos sociais trabalhistas e tributos de qualquer espécie que venham a ser devidos em decorrência da execução dos serviços contratados.

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

3.6. Treinamento / Transferência de Conhecimento

3.6.1. A CONTRATADA deverá fornecer treinamento oficial do fabricante, para 02 (dois) participantes, com carga horária mínima de 16 (dezesseis) horas, contemplando a perfeita instalação, operação, manuseio, gerenciamento, configuração e utilização dos produtos contemplados neste Termo de Referência;

3.6.2. Estes treinamentos serão realizados em Brasília/DF e a CONTRATADA deverá providenciar as instalações para o treinamento;

3.6.3. O programa para treinamento/ atualização de conhecimento tecnológico deverá ser previamente aprovado pelo CONTRATANTE e eventuais mudanças de conteúdo solicitadas deverão constar no material didático;

3.6.4. Deverá ser disponibilizado material didático impresso e em mídia, sem custo adicional para o CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês);

3.6.5. Deverá ser emitido certificado de participação ao final do curso a cada participante;

3.6.6. O cronograma efetivo do treinamento será definido em conjunto com o CONTRATANTE, após a assinatura do contrato;

3.6.7. Para todos os efeitos, inclusive de emissão do Termo de Recebimento Definitivo, o treinamento faz parte do processo de implantação da solução;

3.6.8. Caso o treinamento/ atualização fornecido não for satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizá-los novamente, sem ônus adicional ao CONTRATANTE.

3.6.9. Este treinamento deverá ser realizado por técnico qualificado e certificado pelo fabricante da solução ofertada.

3.7. Garantia da solução

3.7.1. O prazo de garantia dos produtos é de, no mínimo, 48 (quarenta e oito) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo.

3.7.2. A solução ofertada deve ter prazo de garantia de funcionamento e de direito a atualização de versões enquanto vigorar o contrato firmado entre a licitante e o CJF.

3.7.3. Os custos relativos ao fornecimento da garantia devem ser computados no preço do próprio item referente ao software.

3.7.4. Durante o prazo de garantia, a contratada deverá providenciar, sem ônus adicional para o Conselho, o fornecimento de atualização de versão e/ou release, bem como patches de todos os softwares que integram a solução, incluindo drivers e todos os demais elementos integrantes da solução fornecida.

3.7.5. A garantia consiste, entre outros:

a) Na reparação das eventuais falhas de funcionamento, mediante a substituição de versão, de acordo com os manuais e normas técnicas específicas.

b) Na orientação das melhores práticas de uso do produto adquirido.

c) Todas as atualizações, novas versões e releases do software.

3.7.6. A CONTRATADA deverá disponibilizar a atualização dos produtos licenciados assim que houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;

3.7.7. O direito de atualização de versão de cada programa deverá abranger:

a) Logo após a contratação e sempre que for lançada nova versão ou release de qualquer programa integrante do conjunto de programas, a licitante vencedora deverá enviar ao Conselho, em até 15 dias úteis, um conjunto de mídias de instalação da versão fornecida ou atualizada e nota informativa das funcionalidades implementadas na nova versão. Será aceita a disponibilização das atualizações no sítio do fabricante, como alternativa ao envio das mídias;
b) Download de drivers, firmwares, patches, atualizações dos programas e manuais técnicos, a partir do sítio internet do fabricante do produto;
c) Todas as atualizações, novas versões e releases dos programas que fizerem parte da solução contratada;
d) Direito de acesso pelos técnicos do CJF à base de conhecimento e a fóruns da solução no sítio do fabricante;
e) A contratada deverá notificar o CJF em prazo não superior a dez dias sobre a disponibilidade de novas versões e releases dos softwares que fizerem parte da solução fornecida;
3.7.8. Juntamente com a documentação de instalação da solução, como requisito para o aceite definitivo da solução, a contratada deverá entregar a seguinte documentação:
a) Certificados de garantia de que todos os produtos estão cobertos pela garantia, por todo o período contratado, incluindo as extensões de garantia do fabricante, de forma que sejam atingidos os 48 (quarenta e oito) meses totais exigidos.
b) Caso não seja comercializada extensão de garantia com o prazo ou nos moldes exigidos no item anterior, deverá ser entregue pela contratada uma declaração nesse sentido, fornecida pelo fabricante dos equipamentos ou seu representante legal no Brasil. Nesse caso, a contratada assumirá a resolução dos defeitos eventualmente apresentados pelo software por seus próprios meios durante o período complementar à garantia original, até término do contrato;
c) Cessões de direito de uso perpétuo dos programas fornecidos. Os termos de licenciamento de todos os programas fornecidos, emitidos pelo fabricante, deverão ser entregues pela contratada e os mesmos serão direito pertencentes ao Conselho;
d) Conjunto de direitos de atualização de versão, pelo período de 48 meses de garantia, de todos os programas fornecidos. Abrangerá todos os programas e licenças a serem fornecidos. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela contratada e comporão direito pertencente ao patrimônio do Conselho.
3.7.9. A Contratada deverá promover o isolamento, identificação e caracterização de falhas de laboratório (bugs), encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução;
a) Serão consideradas falhas de laboratórios o comportamento ou características dos programas que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados pela CONTRATANTE como prejudiciais ao seu uso.

3.8. Suporte Técnico

3.8.1. Realizar atendimentos "on-site" (Severidade 1 e 2) e remotos (Severidade 3 e 4) conforme categorização definida;
3.8.2. O atendimento deverá ser categorizado em quatro níveis. A contratada deverá garantir tempo máximo de atendimento e restauração de serviço, conforme tabela abaixo:

Criticidade	Descrição	Prazo máximo de atendimento	Prazo máximo para restauração de serviço
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto na operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 1 (uma) hora deve ter um técnico do fornecedor On-site.	Em até 6 horas

Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 2 horas deve ter um técnico do fornecedor On-site.	Em até 10 horas
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Em até 4 horas um técnico do fornecedor entra em contato.	Em até 24 horas
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 72 horas

3.8.3. Na abertura do chamado, a Contratada deverá informar o número da ordem de serviço;
3.8.4. A Contratada deverá enviar mensalmente um relatório consolidado das ordens de serviço geradas no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, os problemas verificados, as recomendações e orientações técnicas;
3.8.5. A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.
3.8.6. A Contratada deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CJF, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações;
3.8.7. A Contratada deverá orientar a CONTRATANTE para, quando for conveniente à CONTRATANTE, proceder à aplicação de pacotes de correção e implantação de versões do produto, cabendo à CONTRATADA orientar e disponibilizar um técnico para contato, em caso de dúvidas ou falhas, por meio telefônico ou correio eletrônico.
3.8.8. O CONTRATANTE fará a "abertura de chamados" técnicos através de ligação telefônica ou via web, em período integral 24 (vinte e quatro) horas por dia 07 (sete) dias por semana. A CONTRATADA deverá informar o número do telefone em sua proposta. Se a Central de Suporte estiver localizada fora de Brasília, a Contratada deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;
3.8.9. A CONTRATADA deverá disponibilizar suporte técnico de toda a solução, através da forma de atendimento remoto, em período integral – 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, pelo período de garantia da solução.

OBRIGAÇÕES DO CONTRATANTE

3.9. Acompanhar e fiscalizar a execução do objeto contratual;
3.10. Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual;
3.11. Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados;
3.12. Comunicar formalmente qualquer anormalidade ocorrida na execução dos serviços pela CONTRATADA;
3.13. Avaliar todos os serviços prestados pela CONTRATADA;
3.14. Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal;
3.15. Indicar os seus representantes para fins de contato e demais providências inerentes à execução do contrato;
3.16. Para os serviços inclusos no período de garantia do objeto, a Contratante permitirá o acesso dos técnicos

habilitados e identificados da CONTRATADA às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àquelas referentes à identificação, trânsito e permanência em suas dependências.

UNIDADE GESTORA/ FISCALIZADORA DO CONTRATO

3.17. O Chefe da Seção de Suporte à Infraestrutura (SESIT) será o gestor do contrato e acompanhará sua execução, devendo proceder a orientação, fiscalização e interdição da sua execução, se necessário, a fim de garantir o exato cumprimento das condições estabelecidas em contrato;
3.18. O representante da Área Administrativa (Fiscal Administrativo do Contrato), indicado pela autoridade competente dessa área, fiscalizará o contrato quanto aos aspectos administrativos, tais como a verificação de regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.

FORMA DE PAGAMENTO

3.19. A CONTRATADA deverá emitir Nota Fiscal/ Fatura somente após a aprovação do CONTRATANTE, ou seja, somente após receber cópia do Termo de Recebimento Definitivo da solução implantada.
3.20. O pagamento do serviço de Suporte Técnico será efetuado mensalmente após envio da fatura pela CONTRATADA.

VIGÊNCIA

3.21. A vigência do Contrato deverá será de 04 (quatro) meses contados da data de sua assinatura, destinados a entrega da documentação, instalação da solução antivírus e transferência de conhecimento.
3.22. A vigência contratual de garantia técnica da solução antivírus deverá ser de 48 (meses) meses contados da data do Termo de Recebimento Definitivo, conforme estabelecido no Termo de Referência.

4. LOCAIS DE ENTREGA E INSTALAÇÃO DOS PRODUTOS

4.1. Como esclarecimento, o parque atual do CONTRATANTE está distribuído em sua Sede e sua Gráfica;
4.2. A entrega e instalação das licenças deverão ser feitas nas dependências relacionadas acima.

5. DAS PENALIDADES

5.1. Pela inexecução total ou parcial das obrigações assumidas a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as seguintes sanções:
5.1.1. Advertência;
5.1.2. Multa de mora no percentual correspondente a 0,5% (zero vírgula cinco por cento), calculada sobre o valor total da contratação, por dia de inadimplência, até o limite de 15 (quinze) dias úteis de atraso no fornecimento de solução de segurança caracterizando inexecução parcial.
5.1.3. Multa compensatória no valor de 10% (dez por cento), sobre o valor contratado, no caso de inexecução total do contrato;
5.1.4. Multa de 5% (cinco por cento) sobre o valor mensal para o serviço de Suporte Técnico, por hora de atraso no caso do descumprimento dos prazos de atendimento, limitado a 30% (trinta por cento) sobre o valor do contrato;
5.1.5. A reincidência da aplicação de multa por 3 (três) meses dará direito ao CJF à rescisão contratual unilateral.
5.2. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

6. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

6.1. A LICITANTE vencedora deverá fornecer declaração comprometendo-se a prestar garantia de, no mínimo, 48 (quarenta e oito) meses a contar da data de recebimento do Termo de Aceite Definitivo;
6.2. A LICITANTE deverá ofertar garantia de atualização contínua pelo período de 48 (quarenta e oito) meses;
6.3. A proposta deverá incluir, em anexo, catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item. Não será aceita proposta sem esta documentação;

6.4. Todos os produtos e as licenças dos softwares especificados deverão ser adquiridos de um mesmo (único) fabricante, em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo com o término do contrato;
6.5. Toda a solução de segurança proposta deverá ser fornecida por um único fabricante de modo que, tanto o suporte à solução quanto as funcionalidades, sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento do mesmo fabricante.
6.6. A LICITANTE vencedora deverá apresentar atestado(s) de capacidade técnica, que comprove que a empresa LICITANTE tenha fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução com complexidade operacional e dimensão equivalente a do CONTRATANTE, especificada neste Termo;
6.7. Deverão constar, preferencialmente, do atestado de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término do contrato e mais dados técnicos com informações sobre o fornecimento/serviço executado.

6.8. Prova de conceito

6.8.1. Poderá ser solicitada prova de conceito à empresa classificada, antes da adjudicação, com o objetivo de realizar testes de comprovação de atendimento às especificações e requisitos exigidos nas Especificações Técnicas deste Termo de Referência;
6.8.2. Para a realização da prova de conceito da solução corporativa antivírus, a LICITANTE deverá disponibilizar e instalar todos os softwares ofertados, nos respectivos sistemas computacionais existentes, exigidos neste Termo de Referência, na Secretaria de Tecnologia da Informação do CJF, localizada no SCES Trecho 03 Polo 08 Lote 09, CEP 70304-902, Brasília – DF, em dias úteis, no prazo de 05 (cinco) dias úteis, contados a partir da data de convocação do CONTRATANTE para a realização da prova de conceito;
6.8.3. O CONTRATANTE, a seu critério, poderá prorrogar a duração da prova de conceito por mais 02 (dois) dias úteis;
6.8.4. Para a avaliação da prova de conceito, o sistema deverá ser instalado pela LICITANTE, na versão a ser fornecida na contratação, em ambiente de homologação do CONTRATANTE, com o acompanhamento de representantes da área gestora e da TI do CONTRATANTE;
6.8.5. A prova de conceito utilizará como base as especificações técnicas constantes neste Termo de Referência;
6.8.6. Será rejeitada a prova de conceito que:
a) Não comprovar o atendimento a no mínimo 01 (um) item descrito no item Especificações Técnicas, deste Termo de Referência;
b) Apresentar divergências em relação às especificações técnicas da proposta.
6.8.7. Não será aceita a proposta da LICITANTE que tiver a prova de conceito rejeitada ou não entregue no prazo estabelecido;
6.8.8. Nesse caso, a proposta subsequente será examinada e, assim, sucessivamente, na ordem de classificação, até a aprovação de uma prova de conceito.

7. DOCUMENTOS ANEXOS

Seguem anexos a este Termo de Referência os seguintes documentos:
1. Anexo I – Especificação Técnica da Solução;
2. Anexo II – Ambiente Tecnológico do CJF;
3. Anexo III – Cronograma de Implantação;
4. Anexo IV – Planilha de Preços.

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

Todas as soluções, independentemente do fabricante, deverão atender as condições, características e especificações técnicas previstas neste Termo de Referência e demais itens não previstos que possam influir direta ou indiretamente no ambiente computacional do CONTRATANTE, bem como nos aspectos de disponibilidade e segurança requeridos neste item;
Toda a solução de antivírus deverá ser compatível com o ambiente tecnológico do CJF (ANEXO II)

2. Características técnicas da solução corporativa de antivírus para gerenciamento, centralização de atualizações, logs e criação de relatório:

1.1. Suportar o gerenciamento dos componentes da solução: antivírus para estação/servidores e antivírus de correio eletrônico;
1.2. Permitir integração com Microsoft Active Directory (AD) para acesso a console de administração;
1.3. Identificar através da integração com o Microsoft AD, quais máquinas estão sem o cliente de antivírus instalado;
1.4. Deverá permitir a atualização dinâmica de listas de assinaturas e regras (componentes de segurança) com freqüência diária e horários definidos pelo usuário, no mínimo;
1.5. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir da rede local;
1.6. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;
1.7. Gerar log de auditoria, contendo usuário que acessou a console web e alteração executada;
1.8. Deverá permitir a desinstalação do cliente de antivírus por meio da console de gerenciamento da solução; ou através de ferramenta do próprio fabricante de forma local e remota;
1.9. Permitir remoção de clientes inativos por determinado período de tempo;
1.10. Possibilidade de backup/restore das configurações da solução através da console de gerenciamento;
1.11. Permitir exportação dos relatórios e gráficos para, no mínimo, os seguintes formatos: HTML ou PDF;
1.12. A ferramenta deverá gerar relatórios, estatísticas e gráficos contendo no mínimo os seguintes tipos pré-definidos:
1.12.1. As máquinas que mais receberam ocorrência de vírus;
1.12.2. Os vírus que mais infectaram a rede;
1.12.3. As máquinas que mais infectaram a rede;
1.12.4. Sumário da distribuição da lista de definições de vírus e engines instalados nas estações de trabalho e servidores.
1.13. Permitir criação de templates de relatórios customizados;
1.14. Permitir a deleção dos arquivos em quarentena;
1.15. Deve vir acompanhado de documentação impressa e on-line que contemple instalação, configuração, ativação e uso do produto;
1.16. O software deve ser atualizado gratuitamente, incluindo melhorias e novas versões durante o período de vigência do contrato;
1.17. Gerenciamento centralizado e remoto com interface WEB através de browser (http, https);
1.18. Permitir criação de diversos usuários e perfis para gerenciamento e com diferentes níveis de acesso;
1.19. Atualizar e implementar políticas de segurança para toda a solução, de forma automática, em caso de epidemia, restaurando as configurações originais ao fim da epidemia;
1.20. Permitir criar planos de distribuição das atualizações para plataforma Windows e Linux;
1.21. Ter um serviço de verificação remoto, manual e agendado, que detecte e remova danos causados por vírus do tipo "Trojan Horse";
1.22. Centralização de logs;
1.23. Capacidade de monitorar os serviços de todos os produtos que se reportam para o software de gerenciamento, alertando sobre paradas dos serviços;
1.24. Possuir funcionalidade de single sign-on para login único;

3. Características técnicas da solução corporativa de antivírus e filtro de URL para estações de trabalho e servidores Microsoft Windows:

3.1. A solução de antivírus deverá proteger os seguintes tipos de equipamentos e sistemas operacionais: estações de trabalho fixas e móveis (notebooks) com os sistemas operacionais Microsoft Windows XP Professional, Windows 7, Windows 2003 e 2008 Server (Standard e Enterprise), na plataforma 32 e 64 bits;
3.2. Instalação remota nas estações de trabalho em um único agente, sem requerer outro software ou agente

adicional, previamente instalado;
3.3. Atualização automática das vacinas de forma incremental e da versão do software. O horário de atualização deve ser configurável. A atualização deve permitir conexão através de serviço proxy;
3.4. Desinstalação automática e remota da solução de antivírus proposta e atual na estação;
3.5. Fornecer, em tempo real, o status atualizado das estações de trabalho, com as seguintes informações: data das vacinas, versão do antivírus, nome e IP da máquina;
3.6. Permitir o bloqueio das configurações do cliente, para que não possam ser alterados pelos usuários;
3.7. Geração de backup dos arquivos antes da remoção de vírus;
3.8. Detecção e remoção de vírus de macro em tempo real;
3.9. Notificação automática ao administrador em caso de epidemia de vírus;
3.10. Armazenamento da ocorrência de vírus em log local e em servidor;
3.11. Detecção de vírus no protocolo POP3;
3.12. Proteção contra desinstalação e desativação não autorizada do produto;
3.13. Possibilidade de retorno de versão anterior das vacinas remotamente, a partir da console de gerenciamento;
3.14. Instalação sem necessidade de reiniciar a estação de trabalho;
3.15. Possibilidade de geração de imagens de estação de trabalho com o antivírus, sendo criados números de identificação dos clientes diferentes para imagem gerada;
3.16. Gerenciamento remoto centralizado através de uma console https web;
3.17. Possibilidade de agrupamento das estações de trabalho com configurações específicas para cada grupo e subgrupo;
3.18. Auto-reparo de danos causados por vírus do tipo "trojan horse" de forma automática, sem a necessidade de agentes ou pacotes adicionais. Essa função deve ser nativa da solução, atualizada de forma automática e sem a necessidade da intervenção do administrador;
3.19. Rastreamento de arquivos compactados nos formatos mais utilizados em no mínimo, 10 níveis de compactação;
3.20. Realização de rastreamento real-time, manual e agendado nas estações de trabalho;
3.21. Capacidade para, em caso de epidemia, bloquear acesso às pastas compartilhadas, a portas TCP e UDP, e acesso de escrita e exclusão a diretórios e arquivos específicos;
3.22. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo;
3.23. Realizar ações específicas para cada tipo de código malicioso;
3.24. Possibilidade de colocar arquivos e diretórios em listas de exclusões para não serem verificados pelo antivírus;
3.25. Permitir o reinício automático dos serviços do antivírus caso esse tenha sido parado devido a algum código malicioso, sem a necessidade da intervenção do administrador;
3.26. Capacidade de reservar espaço em disco para atualizações;
3.27. Proteção contra spywares e adwares integrado ao cliente antivírus, sem a necessidade de instalação de agentes ou pacotes adicionais;
3.28. Possibilidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado;
3.29. Permitir configurar quanto de CPU será utilizada para uma varredura manual ou agendada;
3.30. Proteção contra vírus de rede (network vírus) integrado ao cliente antivírus, sem a necessidade de instalação de agentes ou pacotes adicionais, gerenciado de forma centralizada;
3.31. Fornecer notificações caso haja alguma anomalia na rede (IDS, Firewall e/ou vírus de rede);
3.32. A funcionalidade de Firewall e IDS/ IPS deve ser nativa da ferramenta e deve possuir no mínimo:
3.32.1. Suporte aos protocolos TCP, UDP e ICMP;
3.32.2. Reconhecimento dos tráficos DNS, DHCP e WINS, podendo a partir de regras de Firewall executar os bloqueios;
3.32.3. Proteção contra exploração de buffer overflow;
3.32.4. Proteção contra ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;
3.32.5. Possibilidade de agendar a ativação da regra de firewall;
3.32.6. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no "fingerprint" do arquivo;
3.32.7. Deve permitir bloqueio de ataques baseado na exploração da vulnerabilidade;
3.33. Ter mecanismos de proteção dos executáveis de instalação para evitar ataques direcionados para a sua instalação;
3.34. Ter um mecanismo de backup da base de dados da solução, integrada à console de gerenciamento;

3.35. Enviar uma notificação customizada para a fonte da infecção;
3.36. Possuir solução de reputação de páginas web, integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
3.37. Possuir recurso que possibilite ao usuário postergar a varredura agendada;
3.38. Possuir recurso que permita configurar a varredura agendada de acordo com a utilização da bateria do notebook;
3.39. Possuir solução de reputação de arquivos, integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
3.40. Controle de acesso a dispositivos removíveis e periféricos (usb, cdrom etc), com as seguintes opções: acesso total, modificar, leitura e execução, apenas leitura, e bloqueio total;
3.41. Permitir escaneamento dos dispositivos removíveis e periféricos (usb, cdrom etc) mesmo com a política de bloqueio total ativa;
3.42. Permitir criação de usuários com diferentes níveis de administração para facilitar o gerenciamento da ferramenta;
3.43. Integração com o Active Directory para identificar quais máquinas estão no AD e não tem a ferramenta de Antivírus instalada, e assim fazer a instalação para garantir a integridade da rede;
3.44. Fornecer relatório de computadores com serviços da ferramenta não conformes, com versões de componentes inconsistentes, com varreduras desatualizadas e com configurações inconsistentes.
3.45. Permitir que o usuário decida o horário de scaneamento através dos privilégios determinados pelo administrador;
3.46. Permitir autoproteção ao cliente de antivírus em nível de registro, arquivos de programa e processos;
3.47. Proteção contra autorun em USB;
3.48. Possibilitar a utilização de ferramenta prevenção através de ações conhecidas da ameaça antes da criação da vacina.
3.49. Possibilitar o bloqueio a conexões URLs e IPs maliciosos advindas do desktop, com ou sem intervenção do usuário, não somente de acessos via browser, mas de qualquer conexão HTTP;
3.50. O módulo anti-spyware deve estar incluído no produto antivírus;
3.51. A solução de antivírus deve ser integrada ao Windows Security Center, quando utilizado plataforma Microsoft;
3.52. Detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de Tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;
3.53. A solução deve fornecer uma proteção integrada através de somente um agente contra ameaças como virus, trojans, worms de rede, spyware, phishing e rootkits;
3.54. Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:
3.54.1. Processos em execução em memória principal (RAM);
3.54.2. Arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;
3.54.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: ZIP, EXE, ARJ, MIME/UU, Microsoft CAB e Microsoft Compress;
3.54.4. Arquivos recebidos por meio de programas de comunicação instantânea (MSN Messenger, Yahoo Messenger, Google Talk, ICQ, dentre outros);
3.55. Detectar e proteger a estação de trabalho contra ações maliciosas executadas em navegadores Web por meio de scripts em linguagens tais como JavaScript, VBScript/ActiveX, etc;
3.56. Detecção heurística de vírus desconhecidos;
3.57. Permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;
3.58. Permitir diferentes configurações de detecção (varredura ou rastreamento):
3.58.1. Em tempo real de arquivos acessados pelo usuário;
3.58.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
3.58.3. Manual, imediato ou programável, com interface gráfica em janelas, customizável, com opção de limpeza;
3.59. Automáticos do sistema com as seguintes opções:
3.59.1. Escopo: Todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
3.59.2. Ação: somente alertas, limpar automaticamente, apagar automaticamente, ou mover automaticamente para área de segurança (quarentena);

3.59.3. Frequência: diária, semanal e mensal;
3.59.4. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;
3.59.5. Definição do usuário a ser utilizado durante a verificação;
3.60. Gerenciamento local do módulo:
3.60.1. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da Internet, com frequência (no mínimo a cada hora) e horários definidos pelo administrador da solução;
3.60.2. Permitir atualização incremental da lista de definições de vírus;
3.60.3. Atualização automática do engine do programa de proteção a partir de localização na rede local ou na Internet, a partir de fonte autenticável;
3.60.4. Permitir o rollback das atualizações das listas de definições de vírus e engines;
3.60.5. Deve permitir criar planos de distribuição das atualizações para os clientes gerenciados, podendo ter diferentes planos de atualização para diferentes grupos de computadores.
3.61. Gerar registro (log) dos eventos de vírus no servidor;
3.62. Permitir proteção contra parada da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
3.63. Gerar notificações de eventos através de alerta na rede;
3.64. Possibilitar instalação "silenciosa";
3.65. Permitir o bloqueio por nome de arquivo;
3.66. Permitir o travamento de compartilhamentos;
3.67. Permitir o rastreamento e bloqueio de infecções;
3.68. Prover funcionalidade preventiva contra surtos de novos vírus (ataque 'Zero-dia');
3.69. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nos computadores e servidores;
3.70. Efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
3.71. Desinstalar automática e remotamente a solução de antivírus atual bem como a proposta na estação, sem requerer outro software ou agente;
3.72. Deve permitir a desinstalação através da console de gerenciamento da solução;
3.73. Possibilidade de backup/restore das configurações da solução através da console de gerenciamento;
3.74. Possibilidade de backup da base de dados da solução através da console de gerenciamento;
3.75. Permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;
3.76. Possibilidade de determinar a capacidade e o local de armazenamento da área de quarentena;
3.77. Permitir a deleção dos arquivos quarentenados;
3.78. Permitir remoção de clientes inativos em determinado período de tempo;
3.79. Permitir integração com Active Directory para acesso a console de administração;
3.80. Identificar através da integração com o Active Directory, quais máquinas estão sem a ferramenta de antivírus instalada;
3.81. Permitir criação de diversos perfis e usuários para acesso a console de administração.

4. Características técnicas da solução corporativa de antivírus para servidores Linux

4.1. Compatibilidade com o sistema operacional SuSE Linux Enterprise Server 11 ou superior;
4.2. Atualização automática das vacinas de forma incremental e da versão do software. O horário de atualização deve ser configurável. A atualização deve permitir conexão através de serviço proxy;
4.3. Detecção e remoção de vírus, worms, trojans, spywares, adwares e outros tipos de códigos maliciosos, em tempo real, manual, agendada e por meio de varreduras sob demanda;
4.4. Possibilidade de retorno de versão anterior das vacinas remotamente;
4.5. Possibilitar instalação "silenciosa";
4.6. Instalação e configuração sem necessidade de reiniciar o servidor;
4.7. Realização de rastreamento manual e agendado em servidores;
4.8. Armazenamento da ocorrência de malwares em log centralizado ou via syslog;
4.9. Rastreamento de arquivos compactados nos formatos mais utilizados em pelo menos 10 (dez) níveis de compactação;
4.10. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo;
4.11. Possibilidade de colocar arquivos e diretórios em listas de exclusões onde estes não serão verificados

pelo sistema antivírus;
4.12. Permitir executar tarefas a partir de linha de comando;
4.13. Permitir a instalação local via linha de comando e instalação remota;
4.14. Permitir a instalação tanto em servidores quanto em estações Linux;
4.15. Capacidade para, em caso de epidemia, bloquear acesso às pastas compartilhadas, a portas TCP e UDP, e acesso de escrita e exclusão a diretórios e arquivos específicos, restaurando as configurações originais ao término da epidemia, ambos de forma automática através de políticas recebidas do fabricante;
4.16. Proteção contra vírus de rede (network vírus) integrado ao antivírus, sem a necessidade de instalação de agentes ou pacotes adicionais;
4.17. Proteção contra spywares e adwares integrado ao antivírus, sem a necessidade de instalação de agentes ou pacotes adicionais;
4.18. Possibilidade de retorno de versão anterior das vacinas e mecanismo de verificação a partir da console de gerenciamento;
4.19. Gerenciamento remoto através de uma console web;
4.20. Instalação sem necessidade de reiniciar o servidor;
4.21. Possibilidade de colocar arquivos e diretórios em listas de exclusões para não serem verificados pelo antivírus;
4.22. Permitir diferentes configurações de detecção (varredura ou rastreamento):
4.22.1. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
4.22.2. Por linha-de-comando, parametrizável, com opção de limpeza para a plataforma Linux. A ferramenta de antivírus para Linux deve possuir suporte a módulo de kernel dinâmico (Dynamic Kernel Module Support) que permita a compilação do kernel e integração para plataforma Linux.

5. Características técnicas da solução corporativa de antivírus para armazenamento centralizado de dados (Storage):

5.1. A solução deverá ser compatível o Ambiente Computacional do CJF (ANEXO II);
5.2. Deverá possuir compatibilidade com NetApp Data Ontap 7.3.3 ou superior;
5.3. A solução de antivírus deverá possuir a capacidade de negar acesso aos arquivos contaminados;
5.4. A solução de antivírus em seu processo de escaneamento não deverá comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS);
5.5. Deverá permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação o sistema antivírus tomará para arquivos infectados;
5.6. Possibilidade de notificação de eventos e envio de alertas de forma automática para o administrador;
5.7. Armazenamento da ocorrência de vírus em log;
5.8. Possibilidade de funcionamento independente da ferramenta de gerenciamento;
5.9. Possibilidade de retorno de versão anterior das vacinas (rollback);
5.10. Deverá detectar e remover vírus, worms, trojans, spywares, adwares e outros tipos de códigos maliciosos;
5.11. O sistema antivírus deverá permitir conexão de atualização em redes que possuam servidor proxy;
5.12. Permitir atualização automática e de forma incremental da base de dados de vacina;
5.13. Deverá fornecer em tempo real o status atualizado do sistema antivírus com no mínimo as seguintes informações: versão dos arquivos de vírus (update), dos mecanismos de verificação/correção (engine) e dos programas do sistema;
5.14. A solução de antivírus deverá permitir gerenciamento gráfico intuitivo portável a console (gerenciamento remoto) e escaneamento centralizado.
5.15. A solução de antivírus poderá ser executada em um servidor dedicado ou ser executada no próprio Sistema de Gerenciamento e Armazenamento de Dados (NAS).
5.16. Caso a solução de antivírus necessite de um servidor dedicado, a mesma deverá possuir no mínimo os seguintes requisitos:
5.16.1. Deverá permitir a qualquer momento a incorporação de um novo servidor de antivírus a solução para melhoramento do desempenho.
5.16.2. Deverá permitir o escalonamento Round Robin, isto é, se o primeiro servidor de antivírus estiver ocupado, a solicitação é enviada ao próximo servidor disponível.
5.16.3. Uma vez um servidor de antivírus configurado em um Sistema de Gerenciamento e Armazenamento de Dados, a conexão e re-conexão entre eles deverão ocorrer automaticamente.

5.17. A solução de antivírus deverá suportar conexões de no mínimo 10 Gbps (dez gigabit por segundo);
5.18. A solução de antivírus deverá permitir a configuração de escaneamento nas seguintes modalidades:
5.18.1. Escaneamento manual;
5.18.2. Escaneamento em tempo real;
5.18.3. Escaneamento escalonado.
5.19. A solução de antivírus deverá permitir a configuração de uma lista de tipos de extensões predeterminadas pelo administrador do Sistema para os processos de escaneamento.
5.20. A solução de antivírus deverá mover para área específica e/ou negar acesso aos arquivos contaminados que não forem possíveis de serem limpos.
5.21. A solução de antivírus deverá acompanhar as requisições de escaneamento de arquivo e retornar o seu resultado.
5.22. A solução de antivírus em seu processo de escaneamento não deverá comprometer o desempenho computacional do Sistema de Armazenamento e Gerenciamento de Dados (NAS).
5.23. Para melhorar o desempenho, diminuir o tráfego e aumentar a velocidade, o Sistema antivírus deverá permitir ao administrador do Sistema a configuração dos seguintes passos:
5.23.1. Configurar o Sistema de Armazenamento de Dados (STORAGE) para enviar ao Sistema antivírus somente arquivos com as extensões especificadas.
5.23.2. Os arquivos do Sistema de Armazenamento de Dados serão marcados como "limpos" se os mesmos forem escaneados antes e solicitados sem nenhuma alteração.
5.23.3. Os arquivos marcados como "limpos" não deverão ser escaneados novamente pelo Sistema antivírus.
5.24. A solução de antivírus deverá possuir rotinas bem definidas de escaneamento, atualizações e logs de acordo com as seguintes características:
5.25. Escaneamento de vírus para garantir integridade dos dados e ser capaz de detectar e remover vírus conhecidos e desconhecidos.
5.26. A solução de antivírus deverá utilizar escaneamento recursivo para arquivos compactados.
5.27. Deverá permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação o Sistema antivírus tomará para arquivos infectados:
5.27.1. Deixar em quarentena arquivos infectados;
5.27.2. Limpar com backup;
5.27.3. Limpar sem backup;
5.27.4. Excluir arquivo infectado.
5.28. Notificação de eventos e envio de alertas de forma automática para o administrador como resguardo de situação séria, tal como epidemia de vírus ao Sistema de Armazenamento de Dados;
5.29. Armazenamento da ocorrência de vírus em log centralizado;
5.30. Possibilidade de colocar arquivos e diretórios em listas de exclusões onde estes não serão verificados pelo Sistema antivírus;
5.31. Possibilidade de funcionamento e administração independentes de ferramenta de gerenciamento centralizado;
5.32. Gerenciamento remoto e centralizado do Sistema de antivírus;
5.33. Realizar ações específicas para cada tipo de código malicioso;
5.34. Fornecimento de vacina para novos vírus num prazo máximo de 24 (vinte e quatro) horas, a partir do acionamento ao fornecedor;
5.35. Possibilidade de retorno de versão anterior das vacinas;
5.36. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo;
5.37. Permitir o reinício automático dos serviços do antivírus;
5.38. Proteção no mínimo contra códigos maliciosos classificados como vírus, trojan horses, worms entre outros;
5.39. Suporte compreensível com Help inteligente.
5.40. Da remoção:
5.40.1. Detecção e remoção de vírus em tempo real;
5.40.2. Detecção e remoção de malwares, do tipo: Vírus, worms, trojan horses entre outros;
5.40.3. Proteção contra desinstalação e desativação não autorizada do produto.
5.41. Das Atualizações:
5.41.1. Permitir atualização automática e de forma incremental do cartório de vírus e da base de dados de vacina;
5.41.2. Permitir configuração de forma manual para atualizações referentes às mudanças no programa, erros resolvidos e melhorias. Que a periodicidade e o horário das atualizações também possam ser configuráveis;

5.42. O Sistema antivírus deverá permitir conexão de atualização em redes que possuam servidor Proxy;
5.43. Fornecer em tempo real o status atualizado do Sistema antivírus com no mínimo as seguintes informações: Versão dos arquivos de vírus (update), dos mecanismos de verificação/correção (engine) e dos programas do sistema (upgrade);
5.44. Se uma nova atualização for disponibilizada à solução de antivírus, o administrador do sistema poderá apagar as informações no cache do sistema para forçar a aplicação de um novo escaneamento, inclusive aqueles arquivos que foram escaneados com a versão antiga.

6. Características técnicas da solução corporativa de antivírus e anti-spam baseado em servidor de correio eletrônico Postfix:

6.1. Detectar e remover vírus localizados dentro de arquivos anexados a mensagens, ainda no servidor;
6.2. Rastreamento de arquivos compactados nos formatos mais utilizados em pelo menos 10 (dez) níveis de compactação;
6.3. Deverá conter heurísticas de detecção para filtros de conteúdo e SPAM;
6.4. Permitir configurar ações a serem tomadas na ocorrência de vírus, incluindo limpar, remover, mover para área de quarentena;
6.5. Possuir capacidade de enviar e-mails de alerta para o administrador, na ocorrência de vírus;
6.6. Armazenar log de atividades e vírus, com capacidade de fazer pesquisas no log sem utilizar ferramentas de terceiros, e gerar relatórios;
6.7. Atualização automática e incremental da lista de vírus, vacinas e do scan engine;
6.8. A atualização automática deve permitir conexão através de serviço de proxy;
6.9. Possuir recursos de notificação customizáveis para o administrador e usuário (remetente e destinatário) em caso de detecção de vírus;
6.10. Possuir bloqueio de arquivos anexos e mensagens;
6.11. Filtro de e-mail baseado no tamanho, assunto, texto, e domínio;
6.12. No processo de verificação manual agendado ou em tempo real, o antivírus não deve inviabilizar o uso dos serviços disponibilizados no servidor de e-mail.
6.13. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;
6.14. Restrição de conexão SMTP baseado no host ou range de IP;
6.15. Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;
6.16. Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 (vinte) níveis de compactação;
6.17. Possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos no formato Office Open XML – ISO/IEC 29500:2008, utilizando operados lógicos tais como AND, OR, OCCUR, NEAR, (,), [,] e assim por diante;
6.18. Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário ou qualquer outro endereço de e-mail;
6.19. Realizar atualização de forma automática das vacinas de forma incremental e da versão do software. A atualização deve permitir conexão através de serviço proxy;
6.20. Permitir criar filtros definidos pelo tamanho de mensagem;
6.21. Realizar a verificação em arquivos baseado em seu tipo real, independente da extensão apresentada;
6.22. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;
6.23. Permitir criar regras de controle de conteúdo definidos por rotas;
6.24. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;
6.25. Permitir a criação de grupos de usuários para configuração de regras por grupo ou usuário;
6.26. Possibilidade de configurar o "greeting" SMTP;
6.27. Permitir o controle de relay baseado no domínio e/ou endereço IP;
6.28. Permitir entrega de mensagens a servidores específicos baseado no domínio destino da mensagem;
6.29. Permitir limitar o número de destinatários por mensagem;
6.30. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro;
6.31. Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;
6.32. Permitir criar regras distintas para mensagens que entram e saem;
6.33. Capacidade para, em caso de epidemia, bloquear a entrada de determinados emails, baseado nas características de códigos maliciosos, restaurando as configurações originais ao término da epidemia, ambos de

forma automática através de políticas recebidas do fabricante;
6.34. Possibilidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado;
6.35. Realizar a verificação contra códigos maliciosos no corpo da mensagem;
6.36. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;
6.37. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;
6.38. Gerenciamento via console web https;
6.39. Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;
6.40. Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;
6.41. Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;
6.42. Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegar a um número estabelecido como máximo pelo administrador;
6.43. Permitir a verificação de mensagens no protocolo POP3, permitindo configurar que porta TCP será utilizada;
6.44. Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;
6.45. Permitir a criação de White e Black Lists para um melhor ajuste na detecção de SPAMs;
6.46. Permitir categorizar o tipo do SPAM para um melhor ajuste individual e ações, dependendo da sua classificação;
6.47. Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;
6.48. Permitir exclusão automática das mensagens em quarentena;
6.49. Permitir a verificação de endereços IPs para checar a sua legitimidade, sendo:
6.49.1. Realizar a busca em no mínimo 5 bases de dados localizados no site do fabricante;
6.49.2. Não necessitar instalação adicional;
6.49.3. As bases devem ser do mesmo fabricante do software para gateway SMTP;
6.50. Permitir a verificação heurística contra vírus recém lançados, mesmo sem uma vacina disponível;
6.51. Proteção contra Spywares, sem a necessidade de um software ou agente adicional;
6.52. Prevenir contra ataques do tipo Phishing detectando links de internet no corpo das mensagens que apontam para esse ataque;
6.53. Prevenir contra ataques DHA (Directory Harvest Attack);
6.54. Possuir autenticação via TLS (Transport Layer Security);
6.55. Solução deve ser capaz de receber trafego em tls e realizar conexões em TLS para outros servidores;
6.56. Solução tambem deve possibilitar trafego via Secure SMTP;
6.57. Possuir integração com LDAP (Microsoft Active Directory);
6.58. Disponibilizar relatórios gerenciais que podem ser on demand ou agendados;
6.59. Disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;
6.60. Possibilidade de envio do hash de mensagem para rede inteligente e recebimento da resposta se o hash é um spam ou nao detectado pela rede inteligente;
6.61. Possibilidade de envio para rede inteligente colaborativa de hash de IPs que estejam conectando no servidor de modo a bloquear IPs de spammers emergentes ainda não detectados por heuristica e reputação;
6.62. Análise de reputação de URL dentro da mensagem e tomada de ação caso a URL seja maliciosa;
6.63. Ajuste do nível de sensibilidade do bloqueio de mensagens que tiverem links com má reputação;
6.64. Possibilidade de approved list para a checagem de reputação em URLs dentro de mensagens;
6.65. Bloqueio de ataques de bounce através da metodologia Bounce Address Tag Validation;
6.66. Possibilidade de criar bloqueios por bounce address tag validation de acordo com domínios específicos;
6.67. Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail;
6.68. Ter a possibilidade de fazer approved list para domínios em se habilitando o domain keys identified mail;
6.69. Capacidade de checagem por DNS reverso com até 4 diferentes níveis de bloqueio;
6.70. Bloqueio de IPs por reputação validada em rede inteligente colaborativa;
6.71. Possibilidade de exceções ao bloqueio por reputação com base em pais, range de IP ou IP;
6.72. Configurar nível de sensibilidade da reputação de IPs em até 4 níveis;
6.73. Possibilidade de ter blacklist para bloqueio de IPs diretamente;

6.74. Bloqueio de malware empacotado (packed malware) de forma heurística;
6.75. Definição de timeout de conexão SMTP;
6.76. Suporte a ilimitadas conexões SMTP;
6.77. Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console única.
6.78. Capacidade de realizar profiling de IPs que estejam conectando no servidor e tomar ação necessária caso IPs estejam executando ação maliciosa no que diz respeito a spam;
6.79. Capacidade de apresentar uma console web para que os usuários possam verificar mensagens que estejam em quarentena por motivo de spam;
6.80. Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;
6.81. Capacidade de na mesma solução proteger o tráfego pop3;
6.82. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;
6.83. Solução pode ser ofertada em software para linux ou windows ou no formato software appliance;
6.84. Solução não deve ser ofertada em appliance proprietário;
6.85. Solução deve apresentar relatórios criados através de console web;
6.86. Solução não deve ter interação via linha de comando ou prompt de comando, tudo deverá ser feito por console web;
6.87. Solução deve ter templates pré definidos para relatórios de forma a facilitar a geração de relatórios;
6.88. Solução deve ofertar possibilidade de ter domínio mascarado;

ANEXO II - AMBIENTE TECNOLÓGICO DO CJF

A Contratada deverá fornecer a solução (juntamente com a documentação) que seja compatível e adequada obrigatoriamente à infraestrutura tecnológica do Conselho de Justiça Federal, conforme abaixo:

COMPATIBILIDADE COM O AMBIENTE OPERACIONAL CORRENTE

1. SISTEMAS OPERACIONAIS SERVIDORES

1.1. MS-Windows Server 2003 e 2008 Enterprise Edition de 32 bits e 64 bits;
1.2. Suse Linux Enterprise V.11;

2. SISTEMA OPERACIONAL CLIENTE

2.1. MS-Windows XP SP3;
2.2. MS-Windows 7
2.3. Navegadores Web:
2.3.1. Internet Explorer V.7 e superior
2.3.2. Mozilla Firefox V3.5 e superior

3. BANCOS DE DADOS

3.1. Sistema de Gerenciamento de Banco de Dados Oracle Server Standard Edition 10gR2 ou superior, utilizando o character set WE8ISO8859P1.
3.2. Microsoft SQL Server versão 2008 ou superior;
3.3. Documentação: Dicionário de Dados preenchido no próprio banco de dados, com definição clara e precisa sobre os elementos de dados e Padrão de Nomenclatura utilizado pela empresa.

4. SERVIDORES DE APLICAÇÃO

4.1. Apache 2.2.8 / PHP 5.2.5;
4.2. Compatível com a tecnologia JavaEE ou superior executando em runtime Java JRE/JDK 6 ou superior.

5. SERVIDOR DE AUTENTICAÇÃO

5.1. Compatível com o protocolo Lightweight Directory Access Protocol, ou LDAP.

6. SERVIDORES DE REDE (Características Técnicas)

6.1. Fabricante/Modelo: Dell / Lâminas Power Edge M600
6.2. Memória: 32 GB RAM
6.3. Processador: Intel Xeon X5460 3.16GHz
6.4. Sem disco rígido
Obs: Os servidores serão disponibilizados em máquinas virtuais configurados e dimensionados para atender os requisitos de cada demanda.

7. SOLUÇÃO DE VIRTUALIZAÇÃO

7.1. XenServer versão 5.6.

8. CERTIFICAÇÃO DIGITAL

8.1. Certificado Digital Padrão ICP-Brasil.

AMBIENTE TECNOLÓGICO DO CJF

1. Princípios

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

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

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

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

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

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

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

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

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

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

1.2. A empresa contratada deverá prestar os serviços considerando o ambiente atual do CJF, composto das seguintes tecnologias, entre outras:

2. PLATAFORMA DE HARDWARE

Encontra-se descrito no quadro abaixo, a infraestrutura de hardware em uso no CJF:

Tipo do Ativo	Marca / Modelo do Ativo	Descrição	Quantidade
Servidores Rack	IBM / RS6000	Servidor 4GB HD, 1 GB de memória, 1 Processador RISC Power4, 1 Unidade Fita DAT	1
	IBM RISC pSeries p630 - 7028-6C4	Servidor 4x 36GB HD, 12 GB de memória, 4 Processadores RISC Power4+, 1 Unidade fita DAT	2
	IBM / xSeries 236	Servidor 6x86GB HD, 3 GB de memória, 2 Processadores Xeon, 1 Unidade Fita DAT	1
Videoconferência	Radvsion / Scopia 24	Unidade de Controle Multiponto (MCU)	2
	HP / DL160	Servidor 4GB HD, 4 GB de memória, 2 Processadores Xeon Quad Core	4
	Sony / PCS-G50	Equipamento de videoconferência (Codec)	25
Servidores Blade	Dell / PowerEdge M600	Servidor de dois processadores de núcleo quádruplo com 32GB de RAM	22
	Dell / PowerEdge M610	Servidor de dois processadores de núcleo quádruplo com 32GB de RAM	5

Tipo do Ativo	Marca / Modelo do Ativo	Descrição	Quantidade
Storages	NetApp / FAS3140	2 Controladoras e uma capacidade de 70T bruto sendo 9 shelves com discos FC e SATA. Suporte para FCP, NFS, HTTP	1
	NetApp / FAS2040	2 Controladoras e uma capacidade de 40T bruto sendo 3 shelves com discos FC e SATA. Suporte para FCP, NFS, HTTP	1
Tape Library (Bibliotecas Robotizadas)	IBM / TS3310	Biblioteca composta por 2 drives, com capacidade para 30 fitas LTO3, conexão via Fibre Channel.	1
Racks de Servidores	Dell 42U	Racks p/Servidores/Libraries/Unid. Fita	2
	NetApp 42U	Racks p/Servidores/Libraries/Unid. Fita	1
	Black Box 40U	Racks p/Servidores/Libraries/Unid. Fita	3
Racks de Comunicação	Embratel 40U	Rack 40U p/Ativos de Rede	1
	Furukawa 40U	Rack 40U p/Ativos de Rede	1
Switches Fibre Channel (FC)	EMC / MP8000B	2 switchs FcoE topo de rack com 32 portas sendo 8 de 8Gb/s e 24 de 10Gb/s para rede local Storage/Blade	2
Switches de Core	H3C / S7506E	Concentradores da Rede Local 48 Portas Ethernet 10/100/1000 Mbps, 2 módulos de comunicação 10GB com 8 portas cada, 2 módulos Compat Flash com 2 portas 10GB	2
Switches de Acesso	H3C / S5500	Switchs ethernet 24 portas 10/100/1000 Mbps com Uplink 10Gbps e alimentação redundante	29
Controlador Rede Wireless	3com / WX2200	Switch para Gerência Wireless com 3 portas	1
Access Points (APs)	3com / AP3950	Acesso Rede Wireless 802.11a/b/g/n	25
Equipamentos da Solução Segurança	Fortigate 1000A	Segurança UTM composta de 2 Fortigate com 10 portas 1000Mbps e 1 FortiAnalizer para gravação de logs	3

Tipo do Ativo	Marca / Modelo do Ativo	Descrição	Quantidade
Estações de Trabalho (Desktops)	HP/COMPAQ / DC5750	Processador AMD64 e 1GB de Memória Ram	60
	HP/COMPAQ DC7900	Processador Intel Core 2 duo e 2GB de Memória Ram	300
		Processador Intel i5 Core 2 duo e 4GB de Memória Ram	50
Monitores de Video (LCD)	LG, Dell, Samsung	Monitores de de 17", 19", 21" e 22"	440
Notebooks	Lenovo Thinkpad	Processador Intel centrino com 1GB de Memória Ram	30
	Em processo de aquisição	Processador Core 2 duo com 4GB de Memória Ram	20
Impressoras Laser Monocromáticas	Lexmark E450 e Lexmark T640		60
Impressoras Laser Coloridas	Lexmark C534		30
Impressoras Multifuncionais	Samsung SCX6320		30
Scanner de mesa	Fujitsu e HP		14
Leitoras Código Barras	Bitazec e Symbol		24

3. PLATAFORMA DE SOFTWARE

O quadro a seguir apresenta os Sistemas Operacionais, Aplicativos, Softwares de Gerência, SGBDs, Servidores de Aplicação, Servidores Web e Ferramentas em uso no CJF:

Software	Nome / Versão	Descrição
Sistema Operacional	MS / Windows 2003 e 2008 Server.	Sistema Operacional de 32 bits e 64 bits
	MS / Windows XP Prof. (Port)	Sistema Operacional de 32 bits
	Suse / Linux 9, 10 e 11	Sistema Operacional de 32 bits
	IBM AIX 6.1	Sistema Operacional de 32 bits
Servidores Aplicações	IIS 6.0(Internet Information Services);	Servidor de Aplicações Microsoft ASP / HTML
	Apache 2.2.15	Servidor de Aplicações Apache / PHP
	Tomcat 5	Servidor de Aplicações Java
	OAS 10g	Servidor de Aplicações Oracle
	Plone / Zope	Servidor de Aplicações Zope
	Jboss 4.2.3	Servidor de Aplicações Jboss Java
Aplicativos	MS / Office 2007	Suite de Aplicativos para Escritório
	Internet Explorer # 7	Software de Navegação Internet (Browser)
Softwares / Ferramentas de Gerência / Administração / Monitoração	PHPLDAPADMIN 1.2.0.5	Ferramenta de Administração de Open LDAP
	WEBMIN 1.350	Ferramenta de Administração de Servidores
	AWSTATS 6.7	Ferramenta de Estatística de Sites
	ZABBIX 1.8.2	Software de Monitoramento do Ambiente
	TSM - Tivoli Storage Manager 5.5	Software de Gerenciamento de Backup
	SPAMASSASSIM / MailScanner 4.78.17	Ferramenta de Antispam
	Fortigate 1000A	Solução de Segurança para Rede Corporativa (Firewall, IPS, Filtro de Conteúdo Web, VPN)

Software	Nome / Versão	Descrição
	XenCenter 5.5	Ferramenta de Virtualização de Servidores
	OfficeScan 10.5	Solução de antí-virus
	Jabber – OpenFire 3.6.4	Administração Chat
	Cacti 0.8.7b	Ferramenta de Estatística de Utilização de Rede
	Windows Media Services 9.0	Serviço de Streaming de Video
	Metaframe Presentation Server 4.0	Ferramenta para Acesso Remoto
Gerenciador de Banco de Dados e ferramenta ETL	Postgres 8.1.9	Sistema gerenciador de banco de dados Postgres
	MySql 5.0.26	Sistema gerenciador de banco de dados MySql
	SqlServer 2008	Sistema gerenciador de banco de dados SqlServe
	Ingres II 10.0.0	Sistema gerenciador de banco de dados Ingres
	Brs 8.0	Sistema gerenciador de banco de dados Brs
	Oracle 10g e 11g	Sistema gerenciador de banco de dados Oracle
	ODI 10 / Sunopsis	Ferramentas ETL Oracle Data Integrator e Sunop
Solução de Gerenciamento de Identidades e Controle de Acesso	Novell Identity Manager 2.7 Novell Access Manager 2.6.0 Novell iManager 2.7.0 Provisioning Module for Novell Identity Manager 2.7	Solução de Gerenciamento de Identidades e Controle de Acesso
Servidores Web	IIS 6.0(Internet Information Services);	Servidor de Web
	Apache 2.2.15	Servidor de Web
	Tomcat 5	Servidor de Web
	Jboss 4.2.3	Servidor de Aplicações Jboss.org
	OAS 10g	Servidor de Web
	IMAP 4.1.3	Servidor de POP IMAP Courier

Software	Nome / Versão	Descrição
	PostFix 2.4.3	Servidor de SMTP
	Squid 3.1.1	Servidor de Webcache
	Open LDAP	Servidor de Diretórios
	Dansguardian 2.9.8.0	Servidor de Bloqueio de Conteúdo

ANEXO III
CRONOGRAMA DE IMPLANTAÇÃO

Prazo Máximo (em dias corridos)	Cronograma de Atividades da Prestação dos Serviços	Responsável
D	Assinatura do contrato.	CJF/CONTRATADA
D + 1	Reunião de planejamento.	CJF/CONTRATADA
D + 5	Entregar o Plano Executivo contendo o planejamento para a implantação da solução de segurança. O Plano Executivo deverá dispor sobre o cronograma para instalação, configuração, testes, validação, documentação e treinamento, indicando os principais riscos e forma de mitigação.	CONTRATADA
D + 5	Comprovar que os técnicos envolvidos nos procedimentos e atividades de implantação são certificados pelo fabricante da solução de segurança.	CONTRATADA
D + 10	Aprovar o Plano Executivo para a implantação da solução de segurança.	CJF
D + 15	Entrega do software e das documentações a seguir: a) Documentação oficial do fabricante comprovando a aquisição de licenças juntamente com a garantia da solução de segurança por 48 meses. b) Documentação com identificação e senha que permitam a abertura de chamados técnicos e download de novas versões por meio do sitio internet do fabricante e de telefone.	CONTRATADA
D + 30	Emitir o Termo de Recebimento Provisório após a entrega do software e das documentações.	CJF
D + 45	Finalizar o serviço de implantação da solução corporativa de antivírus, com o funcionamento perfeito de todos os softwares, em sua última versão. Realizar a transferência de conhecimento e entregar toda documentação técnica dos procedimentos executados no serviço de implantação/ migração.	CONTRATADA
D + 60	Emitir o Termo de Recebimento Definitivo após a finalização dos serviços de instalação, configuração e treinamento, acompanhado da documentação técnica detalhada de todos os procedimentos executados.	CJF

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO IV

PLANILHA DE PREÇOS

DESCRIÇÃO	Qtd.	Descrever os nomes dos produtos que compõe a solução	Preço Unitário	Preço Total
1. Licença de uso do software com garantia de 48 meses, composto por:				
Licenças para estações de trabalho Windows	450	McAfee Endpoint Protection – Advanced Suite	R$ 80,00	R$ 36.000,00
Licenças para servidores Windows	30	McAfee Endpoint Protection – Advanced Suite	R$ 65,00	R$ 1.950,00
Licenças para servidores Linux	90	McAfee Endpoint Protection – Advanced Suite McAfee Virus Scan Enterprise for Linux	R$ 65,00	R$ 5.850,00
Licenças para storage	02	McAfee Virus Scan Enterprise for Storage	R$ 2.000,00	R$ 4.000,00
Licenças para servidor de correio eletrônico	01	McAfee E-mail Gateway McAfee E-mail Security	R$ 15.000,00	R$ 15.000,00
Console de Gerência da solução	01	McAfee Endpoint Protection – Advanced Suite McAfee e-Policy orchestrator	R$ 3.683,00	R$ 3.683,00
VALOR TOTAL LICENÇAS DE SOFTWARE				**R$ 66.483,00**
1. Suporte Técnico	48	Para todos os produtos acima	R$ 300,00	R$ 14.400,00
2. Serviços de instalação, configuração e implantação da solução	01	Para todos os produtos acima	R$ 5.000,00	R$ 5.000,00
3. Treinamento / Transferência de conhecimento	02	Para todos os produtos acima	R$ 5.000,00	R$ 10.000,00
VALOR TOTAL SERVIÇOS				**R$ 29.400,00**
VALOR DO CONTRATO				**R$ 95.883,00**