PROCESSO Nº 50840.000.093/2014
CONTRATO ADMINISTRATIVO Nº 14/2014

CONTRATO ADMINISTRATIVO Nº 14/2014, QUE ENTRE SI CELEBRAM A EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A. - EPL E A EMPRESA FAST SECURITY TECNOLOGIA DA INFORMAÇÃO LTDA - ME.

A EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A – EPL, Empresa Pública Federal, vinculada ao Ministério dos Transportes, com sede no Edifício Parque Cidade Corporate - Torre C, SCS Quadra 9, Lote C, 7º e 8º andares, em Brasília/DF, CEP 70.308-200, inscrita no CNPJ sob o n.º 15.763.423/0001-30, e Inscrição Estadual GDF nº 07.622.898/001-15, doravante denominada CONTRATANTE, neste ato representado por seu Diretor-Presidente, Sr. **PAULO SÉRGIO OLIVEIRA PASSOS**, brasileiro, casado, economista, portador da RG nº 671890 SSP/BA e do CPF n.º 128.620.881-53, nomeado pela Ata da 15ª Reunião Ordinária realizada em 29 de novembro de 2013, e pelo Diretor Sr. **HÉLIO MAURO FRANÇA**, brasileiro, casado, advogado, portador da RG nº 297.983, expedida pela SSP/DF e do CPF nº 116.605.701-15, nomeado pela Ata da 2º Reunião Ordinária realizada em 02 de outubro de 2012, e por outro lado a empresa **FAST SECURITY TECNOLOGIA DA INFORMAÇÃO LTDA - ME**, inscrita no CNPJ sob o nº 10.647.012/0001-66, com endereço na SCIA Quadra 14 Conjunto 3 Lote 3 1º andar – Guará – Brasília - DF, CEP 71.250-115, doravante denominada CONTRATADA, neste ato representada pelo seu procurador **GUSTAVO LIMA MIRANDA**, brasileiro, portador da Carteira de Identidade nº 1.828.256 – SSP/DF e do CPF sob o nº 707.868.101-06, resolvem celebrar o presente Contrato, em conformidade com o que consta do Processo Administrativo nº 50840.000.093/2014 - EPL, referente a adesão ao Pregão Eletrônico por Registro de Preços nº 33/2013-COLOG – USG: 160069 do Comando Logístico do Exército e com fundamento na Lei nº 8.666/93, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Aquisição de solução de segurança composta por 345 (trezentos e quarenta e cinco) licenças para *software* de antivírus, *antispyware* e *firewall*, com gerenciamento centralizado, incluindo suporte técnico e atualização de versão dos produtos, pelo prazo de **36 (trinta e seis) meses**; incluindo instalação, conforme quantidades e especificações constantes do Anexo "A".

1.2. Os serviços realizados pela CONTRATADA em desacordo com a origem por ela declarada não serão aceitos, cabendo as penas administrativas legais previstas na legislação.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. Este Contrato guarda conformidade com o Edital do Pregão Eletrônico SRP nº 33/2013 – UASG: 160069, do Comando Logístico do Exército e seus Anexos, vinculando-se, ainda, à Proposta da CONTRATADA e demais documentos constantes do Processo nº 50840.000.093/2014 – EPL que, independente de transcrição, integram este Instrumento.

2.2. O objeto deste contrato decorre de adesão à Ata de Registro de Preços correspondente ao item 6 do Pregão Eletrônico SRP nº 33/2013 – UASG: 160069, do Comando Logístico do Exército – COLOG.

CLÁUSULA TERCEIRA – DOS PREÇOS

3.1. Os preços unitários e totais do lote que constitui o objeto deste contrato, já incluídas as despesas de frete, impostos, seguro, embalagem e outras decorrentes, são os seguintes:

Item	Descrição	Quantidade	Valor Unitário*	Valor Total da Contratação
01	Licenças de uso perpétuo de software (antivírus), com suporte técnico e atualização de versão por 36 (trinta e seis) meses, incluindo instalação.	345	R$ 90,00	R$ 31.050,00

*Valor correspondente ao item 6 da Ata de Registro de Preços do Comando Logístico do Exército – UASG: 160069 – Pregão por Registro de Preços nº 33/2013 - COLOG.

3.2. O valor do contrato é de **R$ 31.050,00 (trinta e um mil e cinquenta reais)**.

CLÁUSULA QUARTA – DO PAGAMENTO

4.1. O pagamento será realizado em até **30 (trinta) dias** após o adimplemento, aceitação e apropriação da solução de segurança entregue pela CONTRATADA, mediante o recebimento, na CONTRATANTE, de 02 (duas) vias da nota fiscal com o recebimento atestado no verso pelo fiscal do contrato; 01 (uma) cópia da CNDT (Certidão Negativa de Débitos Trabalhistas) e o respectivo Termo de Recebimento Definitivo.

4.2. A nota fiscal deverá ser emitida sem rasura, em letra legível, em nome da EPL, informando o número, agência, conta bancária e o nome do banco.

4.3. Havendo erro na nota fiscal que impeça o pagamento da despesa, aquela será devolvida à CONTRATADA e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação ou representação do documento fiscal, não acarretando qualquer ônus para a CONTRATANTE.

CLÁUSULA QUINTA - FORMA DE FORNECIMENTO

5.1. O objeto deste contrato deverá ser entregue de acordo com os prazos constantes da Cláusula Sétima.

CLÁUSULA SEXTA – DA GARANTIA DE EXECUÇÃO DO CONTRATO

6.1. A execução deste contrato está assegurada por 36 meses no valor de R$ 1.552,50 (um mil quinhentos e cinquenta e dois reais e cinquenta centavos),

correspondente a 05 (cinco) por cento do valor total da contratação, com validade de no mínimo 60 (sessenta) dias após a data limite prevista para o término da vigência deste contrato, de acordo com o art. 56 da Lei 8.666/93.

6.2. A liberação da garantia prestada será feita, após o cumprimento integral deste contrato, comprovado pelo recebimento definitivo de seu objeto, por comunicação expressa da CONTRATANTE.

CLAÚSULA SÉTIMA – DAS CONDIÇÕES DE RECEBIMENTO

7.1. Os *softwares* da solução de antivírus deverão ser instalados na Sede da CONTRATANTE, localizada no Edifício Parque Cidade Corporate - Torre C, SCS Quadra 9, Lote C, 7º e 8º andares, Brasília/DF, CEP 70.308-200, em até **45 (quarenta e cinco) dias**, a partir do recebimento da nota de empenho, correndo por conta do fornecedor todas as despesas decorrentes.

7.2. A CONTRATADA será responsável pela substituição, troca ou reposição dos produtos se, em até **15 (quinze) dias**, porventura, forem entregues com qualquer natureza de defeito, avaria ou não compatíveis com as especificações deste Contrato.

7.3. A CONTRATADA realizará treinamento para utilização do produto, a ser ministrado na cidade de Brasília-DF, para, no mínimo, 08 (oito) técnicos indicados pela CONTRATANTE, com 12 (doze) horas de duração, em data e horários estabelecidos pela CONTRATANTE.

7.4. Serão observados o prazo de garantia dos serviços executados.

7.5. Após a instalação dos componentes da solução de antivírus contratada, conforme as especificações técnicas, a Comissão de Recebimento designada pela CONTRATANTE confeccionará o Termo de Recebimento Definitivo (TRD), acompanhado da nota fiscal original, com atesto no verso, para fins de pagamento.

7.6. Em caso de não conformidade com as especificações técnicas constantes deste contrato, a CONTRATANTE notificará a CONTRATADA para sanar os problemas ou para efetuar a reposição de todo o material defeituoso. Caso contrário, a CONTRATADA ficará sujeita às sanções administrativas por deixar de cumprir o estabelecido nas especificações técnicas do produto.

7.7. Caso a CONTRATADA indique que o objeto deste contrato será procedente de país estrangeiro (importado), a CONTRATADA deverá apresentar, como condição obrigatória para o recebimento, a licença e a documentação aduaneira de liberação da importação, junto com a nota fiscal.

7.8. Será rejeitado, no todo ou em parte, o que for fornecido em desacordo com este contrato.

CLÁUSULA OITAVA - DA GARANTIA TÉCNICA

8.1. A garantia dos produtos e da prestação dos serviços de suporte técnico será de **36 (trinta e seis) meses**, contados a partir da data de emissão do Termo de Recebimento definitivo, podendo ser prorrogada.

8.2. A garantia deverá englobar qualquer atividade relacionada ao funcionamento dos produtos, como manutenção evolutiva, preventiva e corretiva em *software*, sem nenhum ônus para a CONTRATANTE.

8.3. Durante o período de garantia, é de responsabilidade da CONTRATADA a atualização de versões dos *softwares* fornecidos.

8.4. A CONTRATADA deverá disponibilizar à CONTRATANTE, sem custo adicional, as respectivas atualizações de versões e "*releases*" de todos os produtos fornecidos, durante o período de garantia e deverá prestar ao Contratante todo o suporte necessário para instalação e configuração das mesmas.

8.5. Durante o período de garantia de atualização técnica, a CONTRATADA deverá entregar as revisões dos manuais técnicos e/ou documentação dos *softwares* licenciados, sem ônus adicionais para a CONTRATANTE.

8.6. As novas versões do objeto contratado deverão ser disponibilizadas em até **05 (cinco) dias** corridos, a partir do lançamento oficial da versão.

8.7. A Contratada garante à CONTRATANTE que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou *trade-secrets*.

8.8. Caso os produtos licenciados venham a ser objeto de ação judicial em que se discuta a infringência de patentes, direitos autorais ou *trade-secrets*, a CONTRATADA garante à CONTRATANTE que assumirá a direção defesa em juízo, responsabilizando-se pelos honorários advocatícios, custas processuais, bem como por todo e qualquer prejuízo.

8.9. PRODUTIVIDADE DE REFERÊNCIA

8.9.1. Os profissionais que efetuarão a instalação, a configuração, implementação e o suporte técnico deverão ser certificados nos produtos adquiridos pela CONTRATANTE.

8.9.2. Os serviços serão executados na Sede da CONTRATANTE e será disponibilizado à CONTRATADA, local e meios materiais tais como: espaço físico, equipamentos, mobiliário, instalações e os meios de comunicação necessários ao desempenho e cumprimento dos serviços.

8.10. ORDEM DE SERVIÇO

8.10.1. Será utilizado o procedimento de abertura de ordem de serviço para as comunicações formais quanto à garantia técnica.

8.10.2. A contratada deverá ofertar um modelo de ordem de serviço para aprovação pela comissão de recebimento, onde constem, no mínimo, os campos descritos abaixo, observando o previsto no Acordo de Nível de Serviço ANS.

a) Descrição do chamado técnico;

b) Data/hora da abertura do chamado técnico;
c) Data/hora de chegada do(s) técnico(s) ao local do serviço;
d) Registro do atendente;
e) Registro do técnico solicitante;
f) Número do ticket referente ao chamado;
g) Registro do grau de severidade do chamado;
h) Avaliação da qualidade do atendimento;
i) Tempo total decorrido para o atendimento do chamado técnico (abertura do ticket à resolução do problema);
j) Tempo total decorrido para a resolução do problema (chegado do técnico ao local do atendimento à resolução do problema);
k) Relatório descritivo do serviço realizado; e
l) Aceite do serviço.

8.10.3. As aberturas das ordens de serviço se darão via 0800, telefone local, site e/ou e-mail específico, devendo essas informações de contato serem fornecidas pela CONTRATADA.

8.10.4. Os atendimentos para aberturas das ordens de serviço deverão estar disponíveis 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

8.11. ACORDO DE NÍVEIS DE SERVIÇO

8.11.1 Procedimentos e critérios de mensuração:

Índice Nº 01 Prazo de atendimento para demandas de Ordens de Serviço (OS) *on-site*	
Item	Descrição
Finalidade	Garantir um atendimento célere e eficiente às demandas de suporte técnico *on-site* da CONTRATANTE, solicitadas por meio de Ordem de Serviço.
Meta a cumprir	Atender as demandas solicitadas por meio de Ordem de Serviço – OS, nos prazos estabelecidos neste índice com a correção do problema, caso necessário.
Método de medição	Cronometragem de tempo que se inicia após o recebimento da confirmação da solicitação da OS e a devida identificação (ticket de abertura), enviado por e-mail e/ou telefone à CONTRATANTE.
Forma de acompanhamento	Acompanhamento presencial do fiscal do contrato ou representante técnico por ele indicado durante a execução da OS até o seu encerramento.
Periodicidade	Mensal
Mecanismo de Cálculo do tempo de	Somatório do número de horas de

execução da OS	efetivo serviço - chegada do técnico da CONTRATADA ao local do atendimento até o final da execução da OS.
Tempo de restabelecimento do problema relatado na abertura da OS.	Após a chegada do técnico da CONTRATADA ao local do atendimento: - Até 02 (duas) horas para grau de severidade alto: e - Até 04 (quatro) horas para grau de severidade baixo.
Tempo esperado de atendimento para situações não críticas (grau de severidade baixo) - TASNC	Até 02 (duas) horas contadas a partir do início da medição até a chegada do técnico ao local de atendimento.
Tempo esperado de atendimento para situações críticas (grau de severidade alto) - TASC	Até 01 (uma) hora contada a partir do início da medição até a chegada do técnico ao local de atendimento.

Continuação do Índice Nº 01
Prazo de atendimento para demandas de Ordens de Serviço (OS) *on-site*

Item	Descrição
Faixas de ajuste no pagamento - FAP	FAP01 - TASNC e TASC cumpridos dentro do estipulado neste índice, pagamento de 100% do valor da OS. FAP02 - TASC com atraso de 30 (trinta) minutos a 01 (uma) hora do estipulado neste índice, pagamento de 80% do valor da OS. FAP03 - TASNC com atraso de 30 (trinta) minutos a 01 (uma) hora do estipulado neste índice, pagamento de 90% do valor da OS. FAP04 - TASNC ou TASC com atraso superior a 60 (sessenta) minutos do estipulado neste índice, pagamento de 70% do valor da OS.
Sanções	Ocorrências de 02 eventos FAP02 por mês, multa de 30% sobre o valor total mensal contabilizado. Ocorrências de 02 eventos FAP03 por mês, multa de 20% sobre o valor total mensal contabilizado. Ocorrências de 02 eventos FAP04 por mês, multa de 40% sobre o valor total mensal contabilizado. Ocorrências de mais de 02 eventos FAPs quaisquer por mês, advertência na forma da lei. No caso de reincidência do parágrafo anterior, rescisão contratual, em conformidade com os procedimentos legais vigentes no COLOG.

Observações	- Às sanções aplicadas, se somarão os ajustes de pagamento (cumulativamente); - Os atrasos deverão ser informados no relatório descritivo do serviço realizado na OS.

CLÁUSULA NONA – DO FISCAL DO CONTRATO

9.1. A CONTRATANTE nomeará empregados para fiscalização deste contrato, obrigando-se a CONTRATADA a facilitar, de modo amplo e irrestrito, a ação dos mesmos.

9.2. Serão previstas, a critério da CONTRATANTE, visitas técnicas às instalações da CONTRATADA onde se processar a execução dos serviços contratados.

9.3. A CONTRATANTE se reserva ao direito de, sem que de qualquer forma restrinja a plenitude da responsabilidade da CONTRATADA, exercer a mais ampla e completa fiscalização sobre o objeto contratado, cabendo-lhe, entre outras providências de ordem técnica, conferir o serviço fornecido e atestar as notas fiscais, observado o que consta deste contrato e no Acordo de Nível de serviço – ANS.

CLÁUSULA DÉCIMA– PRORROGAÇÃO DO PRAZO DE ENTREGA

10.1. Os prazos de entrega poderão ser prorrogados, desde que ocorra um dos seguintes motivos:

10.1.1. alteração das especificações pela contratante;

10.1.2. ocorrência ou superveniência de fato excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições de execução deste contrato;

10.1.3. interrupção da execução deste contrato ou diminuição do ritmo de trabalho por ordem e no interesse da contratante;

10.1.4. aumento das quantidades inicialmente previstas neste contrato em até 25 % (vinte e cinco por cento) do seu valor inicial atualizado, conforme limites permitidos pelo art. 65 da Lei nº 8666/93, em sua redação atual;

10.1.5. impedimento de execução deste contrato por ato ou fato de terceiro reconhecido pela contratante em documento contemporâneo a sua ocorrência; e

10.1.6. omissão ou atraso de providências a cargo da contratante, inclusive quanto aos pagamentos previstos de que resulte diretamente impedimento ou retardamento na execução deste contrato. (Decreto nº 7.845/2012).

10.2. Verificado algum dos motivos relacionados, a contratante poderá conceder a prorrogação necessária, desde que o respectivo pedido seja apresentado pela

contratada e, mediante petição por escrito, devidamente fundamentado e protocolada na CONTRATANTE, até 10 (dez) dias antes do vencimento do prazo contratual.

CLÁUSULA DÉCIMA PRIMEIRA – PENALIDADES

11.1. O não cumprimento das obrigações contratuais sujeitará à empresa, garantida prévia defesa, às seguintes sanções:

11.1.1. advertência;

11.1.2. multa de mora de 0,1 % (um décimo por cento) calculada sobre o valor do contrato, por até 90 (noventa) dias de atraso injustificado na execução dos serviços (cobrada por dia de atraso);

11.1.3. multa de mora de 0,2 % (dois décimos por cento) calculada sobre o valor do contrato de 90 (noventa) a 180 (cento e oitenta) dias de atraso injustificado na execução dos serviços (cobrada por dia de atraso);

11.1.4. multa de mora 0,3 % (três décimos por cento) calculada sobre o valor do contrato , acima de 180 (cento e oitenta) dias , por dias de atraso injustificado na execução dos serviços (cobrada por dia de atraso);

11.1.5. multa de 0,1 % (um décimo por cento) sobre o valor do contrato por dia de atraso injustificado pela reapresentação do material rejeitado, depois de esgotado o prazo fixado para substituição, correção ou reparação; e

11.1.6. multa de 30% (trinta por cento) sobre o valor do contrato, em caso de rescisão causada por ação ou omissão injustificada da contratada.

11.2. Ficará impedida de licitar e contratar com a União e descredenciada no SICAF, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas neste contrato e demais cominações legais, a aquele que:

11.2.1. deixar de entregar documentação exigida neste contrato ou apresentar documentação falsa;

11.2.2. ensejar o retardamento da execução do objeto da licitação;

11.2.3. não mantiver a proposta;

11.2.4. falhar ou fraudar na execução do contrato;

11.2.5. comportar-se de modo inidôneo;

11.2.6. fizer declaração falsa; ou

11.2.7. cometer fraude fiscal.

11.3. As multas poderão ser aplicadas concomitantemente com as demais sanções, facultada a defesa prévia do interessado no prazo de 05 (cinco) dias úteis, contados a partir da data em que tomar ciência.

11.4. Para efeito de aplicação de multa, o valor do contrato será apurado deduzindo-se dele o valor das entregas realizadas dentro do prazo pactuado e aceitas pela CONTRATANTE.

11.5. A aplicação das sanções previstas neste contrato não exclui a possibilidade da responsabilidade civil da CONTRATADA por eventuais perdas e danos à Administração Pública.

11.6. A multa, aplicada após regular processo administrativo, será descontada da garantia do respectivo contratado.

11.7. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CONTRATANTE ou ainda, quando for o caso, cobrada judicialmente.

CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES

12.1. Obrigações da CONTRATANTE:

12.1.1. Acompanhar e fiscalizar a execução do objeto contratual;

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

12.1.3. Estabelecer normas e procedimentos de acesso às suas instalações para a execução de serviços;

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

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

12.1.6. Avaliar todos os serviços prestados pela CONTRATADA;

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

12.2. Para os serviços de suporte técnico, o CONTRATANTE permitirá o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações onde se encontrarem os equipamentos. Estes Técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àquelas referentes à identificação, trânsito e permanência em suas dependências.

12.3. Caso se interrompa a prestação dos serviços contratados, a área de TIC deverá ter um plano de ação emergencial, de modo a amenizar os problemas surgidos. Este plano deverá ser elaborado juntamente com a equipe da CONTRATADA, devendo abordar em seu conteúdo procedimentos básicos para a execução dos serviços.

12.4. Obrigações da CONTRATADA:

12.4.1. Salvaguardar as informações relativas à execução do contrato com a EPL; não utilizar da presente contratação para obter qualquer acesso não autorizado à informações da EPL; e não veicular publicidade acerca desta contratação, sem prévia autorização, por escrito, da EPL;

12.4.2. Assumir inteira responsabilidade pela entrega do objeto contratado;

12.4.3. Executar o objeto contratado de acordo com as especificações, não sendo aceitas quaisquer modificações sem a expressa autorização, por escrito, do Fiscal deste Contrato;

12.4.4. Submeter à aprovação da CONTRATANTE toda e qualquer alteração ocorrida nas especificações, em face das imposições técnicas, de cunho administrativo, de implementos tecnológicos ou legais indispensáveis à perfeita execução dos serviços;

12.4.5. Sujeitar-se à fiscalização da CONTRATANTE no tocante à verificação das especificações técnicas, prestando os esclarecimentos solicitados, atendendo às reclamações procedentes, caso ocorram, e prestando toda assistência técnica operacional;

12.4.6. Acatar todas as orientações do Fiscal do Contrato, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos sobre o objeto contratado e atendimento das reclamações formuladas.

12.4.7. Prestar garantia pelo prazo de **36 (trinta e seis) meses**, contados a partir da data de emissão do Termo de Recebimento Definitivo.

12.4.8. Responsabilizar-se por quaisquer danos no prejuízos causados por seus empregados aos equipamentos, instalações, patrimônio e bens da CONTRATANTE, em decorrência da execução dos serviços, incluindo-se também os danos materiais ou pessoais a terceiros, a que título for. A CONTRATANTE estipulará o prazo para a reparação dos danos e prejuízos causados.

12.4.9. Manter disciplina nos locais de entrega do objeto contratado, retirando, de imediato, qualquer empregado cuja atuação, permanência e/ou comportamento seja considerados inconvenientes ou insatisfatórios ao interesse do Serviço Público.

12.4.10. Manter, durante a vigência deste contrato, às condições de habilitação para contratar com a Administração Pública, apresentando, sempre que exigido, os comprovantes de regularidade fiscal.

12.4.11. Cuidar para que todos os privilégios de acesso a sistemas, informações e recursos da CONTRATANTE sejam revistos, modificados ou revogados quando da transferência, remanejamento, promoção ou demissão de profissionais sob sua

responsabilidade, em casos de paralização dos transportes coletivos, bem como nas situações nas quais se faça necessária a execução dos serviços em regime extraordinário.

12.5. À CONTRATADA cabe assumir a responsabilidade por:

12.5.1. Todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com a CONTRATANTE;

12.5.2. Todas as providências e obrigações estabelecidas na legislação especificam de acidentes de trabalho, quando em ocorrência da espécie, forem vítimas os seus empregados durante a execução deste contrato, ainda que acontecido em dependência da CONTRATANTE; e

12.5.3. Comprovação da origem dos bens importados oferecidos, e da quitação dos tributos de importação a eles referentes, que deverá ser apresentado no momento da entrega do objeto, sob pena da rescisão contratual e multa.

12.6. São expressamente vedadas à CONTRATADA:

12.6.1. a veiculação de publicidade acerca deste contrato, salvo se houver prévia autorização da Administração do CONTRATANTE; e

12.6.2. a subcontratação de outra empresa para a execução do objeto deste contrato.

CLÁUSULA DÉCIMA TERCEIRA - RESCISÃO

13.1. Este contrato poderá ser rescindido se ocorrer um dos casos previstos no art.78 da Lei nº 8.666/93 que, de alguma forma, comprometa ou torne duvidoso o cumprimento das obrigações assumidas.

13.2. A inexecução total ou parcial deste contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento, conforme dispõe o art. 77 da Lei 9.666/93.

CLÁUSULA DÉCIMA QUARTA – ALTERAÇÃO CONTRATUAL

14.1. Qualquer alteração neste contrato será feita por termo aditivo e obedecerá a formalidade deste contrato e a legislação vigente, em especial o artigo 65 da Lei nº 8.666/93.

CLÁUSULA DÉCIMA QUINTA – ACRÉSCIMO OU SUPRESSÃO DO OBJETO

15.1. A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, o acréscimo ou supressão que se fizer no objeto deste contrato até 25 % (vinte e cinco) por cento do seu valor inicial.

CLÁUSULA DÉCIMA SEXTA – COMUNICAÇÃO

16.1. Qualquer notificação, solicitação ou comunicação que as partes devam enviar uma à outra, em virtude deste contrato, será feita por escrito e considerar-se-á efetuada no momento em que o documento for entregue ao destinatário nos endereços abaixo indicados:

16.1.1. CONTRATANTE:

EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A – EPL
Endereço: Setor Comercial Sul, Lote C, Edifício Parque Cidade Corporate, Torre "C", 7º e 8º andares, Brasília-DF – CEP: 70.308-200 Telefone: 3426-3876

16.1.2. CONTRATADA:

FAST SECURITY TECNOLOGIA DA INFORMAÇÃO LTDA (SCIA Quadra 14 Conjunto 3 Lote – 1º Andar 0 "parte A" 0 Guará – Brasília/DF – Telefone (61) 3363-8636 – comercial@fasthelp.com.br

CLÁUSULA DÉCIMA SÉTIMA – HABILITAÇÃO E QUALIFICAÇÃO

17.1. A CONTRATADA obriga-se a manter, durante toda a execução deste contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

CLÁUSULA DÉCIMA OITAVA– CESSÃO OU TRANSFERÊNCIA

18.1. O presente contrato não poderá ser objeto de cessão ou transferência, no todo ou em parte.

CLÁUSULA DÉCIMA NONA - ANEXOS

19.1. Constituem anexos deste contrato, dele fazendo parte integrante:

A - Especificações Técnicas;
B - Nota de Empenho;
C - Proposta da Contratada; e
D – Ata de Registro de Preços.

CLÁUSULA VIGÉSSIMA – VIGÊNCIA

20.1. Este contrato entrará em vigor na data de sua assinatura e vigerá pelo período de **36 (trinta e seis) meses.**

CLÁUSULA VIGÊSSIMA PRIMEIRA – DA DOTAÇÃO ORÇAMENTÁRIA

21.1. As despesas decorrentes desta contratação correrão à conta da Dotação Orçamentária da União, Programa de Trabalho nº 26.122.2126.2000.0001, Elemento de Despesa 3390.

Empresa de Planejamento e Logística S.A. Fls. 356 Rubrica EPL

CLÁUSULA VIGÉSSIMA SEGUNDA – DOS CASOS OMISSOS

22.1. Os casos omissos serão resolvidos com base nas disposições constantes da Lei nº 8.666/93, dos princípios de Direito Público, aplicando-se, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado.

CLÁUSULA VIGÉSIMA TERCEIRA - PUBLICAÇÃO

23.1. O extrato deste contrato será publicado no Diário Oficial da União, conforme previsto no parágrafo único, art. 61 da Lei nº 8.666/93.

CLÁUSULA VIGÉSIMA QUARTA – FORO CONTRATUAL

24.1. Fica eleito o foro da cidade de Brasília-DF para dirimir as questões decorrentes da execução deste contrato.

24.2. E, por estarem assim ajustados, firmam as partes o presente instrumento, em 02 (duas) vias de igual teor, juntamente com duas testemunhas.

BRASÍLIA, 25/6/2014

CONTRATANTE:

PAULO SÉRGIO PASSOS
Diretor Presidente
CONTRATANTE

HELIO MAURO FRANÇA
Diretor
CONTRATANTE

CONTRATADA:

GUSTAVO LIMA MIRANDA
Representante Legal
CONTRATADA

TESTEMUNHA DA EPL:

Nome: DENIS MARIO REIS DA SILVA
CPF: 011 808 681-29
Identidade: 4273813 - DGPC/GO

TESTEMUNHA DA CONTRATADA:

Nome:
CPF: 995.154.311-53
Identidade: 2.167.373 DF

Ricardo Miranda Campos
Núcleo de Tecnologia
Mat. SIAPE [illegible]
EPL

(PELA CONTRATADA)

Empresa de Planejamento e Logística S.A. Fls. Rubrica EPL

ANEXO "A"

ESPECIFICAÇÕES TÉCNICAS

1. Aquisição de Solução de Segurança para Endpoints , com garantia de manutenção e suporte para 36 Meses, conforme características listadas abaixo:

1.1. Toda solução de segurança de antimalware proposta deverá ser fornecida por um único fabricante de modo que tanto o suporte a solução quanto as funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento, via web browser;

1.2. Proteção total de segurança para servidores de rede e arquivos;

1.3. Suporte total aos sistemas operacionais baseados na plataforma Windows: Windows Server 2003 em todas as suas versões, Windows Server 2008 em todas as suas versões;

1.4. Todas as funcionalidades deste item devem ser ativadas por agente único que facilita a instalação, a configuração e o gerenciamento;

1.5. Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções:

1.5.1. Limpar arquivos automaticamente;
1.5.2. Excluir arquivos Automaticamente; e
1.5.3. Negar Acesso aos Arquivos (quarentena).

1.6. Rastreamento manual com interface Windows, customizável, com opção de limpeza;

1.7. Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável;

1.8. Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo;

1.9. Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers, etc;

1.10. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador;

1.11. Permitir atualização incremental da lista de definições de vírus;

1.12. Salvar automaticamente as listas de definições de vírus em local especificado na rede, após cada atualização bem-sucedida;

1.13. Programação de rastreamentos automáticos do sistema com as seguintes opções:

1.13.1. Escopo: Todos os drives locais, drives específicos, ou pastas específicas;

1.13.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

1.13.3. Frequência: Horária, diária, semanal, mensal; e

1.13.4. Exclusões: Pastas ou arquivos que não devem ser rastreados.

1.14. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

1.15. Gerar notificações de eventos de vírus através de alerta na rede;

1.16. Permitir a instalação em ambientes em Cluster Microsoft;

1.17. Permitir bloqueio de aplicações pelo nome do arquivo;

1.18. Possibilidade de reparar o registro do sistema após eliminação de epidemia;

1.19. Permitir bloqueio de portas;

1.20. Permitir criação de regras baseadas em processos de sistema;

1.21. Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia;

1.22. Possuir proteção contra estouro de buffer;

1.23. Capacidade de retomar atualizações de DAT's e de software do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinicio de todo o processo;

1.24. Detecção de *cookies* potencialmente indesejáveis no sistema;

1.25. O sistema de *antispyware* deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca DAT de definições de vírus e demais ameaças;

1.26. Possuir a capacidade de monitorar e bloquear as invasões, combinando proteção comportamental e a proteção por características com um firewall e um único produto;

1.27. O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus, *antispyware*, *antispam* e controle de acesso à rede. Possibilitando uma única e simples interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum

software adicional a console de gerenciamento para permitir o controle integrado;

1.28. Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP;

1.29. Deve possuir o recurso de blindagem, impedindo o comprometimento dos aplicativos e dos seus dados, além de evitar que um aplicativo seja usado para atacar outros aplicativos;

1.30. Possuir proteção, pronta para operação e contra vulnerabilidades desconhecidas, tais como buffer overflow e ataques de dia zero (zero-day attacks);

1.31. Possuir proteção contra BOTs;

1.32. Estar de acordo com as regulamentações GLBA, CA Breach Act 1386, Sarbanes-Oxley e HIPAA;

1.33. Capacidade de trabalhar no modo adaptativo se adaptando a novas aplicações instaladas na máquina;

1.34. Disponibilizar os seguintes relatórios na plataforma de gerencia: sumário de eventos de IPS por assinatura, por alvo, por endereço IP origem, os 10 principais nós atacados, as 10 principais assinaturas, sumário das aplicações bloqueadas e update de quarentena;

1.35. Permitir o bloqueio de ataques baseados em Web como: Directory Traversal attacks e Unicode attacks;

1.36. Interceptar tráfego e requisições de HTTP após decriptação e decodificação;

1.37. Permitir o bloqueio de aplicações e os processos que a aplicação interage;

1.38. Funcionar tanto no ambiente corporativo como em VPN;

1.39. Trabalhar no modo de quarentena permitindo a verificação pelo software de gerenciamento se o cliente está trabalhando com políticas antigas e versões desatualizadas, neste caso, o cliente é bloqueado a uma área de quarentena, limitando o acesso a rede desta estação;

1.40. Capacidade de detectar e bloquear tentativas de invasão;

1.41. Possuir instalação "silenciosa";

1.42. Bloquear acessos indevidos que não estejam na tabela de políticas definidas pelo administrador;

1.43. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;

1.44. Permitir monitoração de hooking de aplicações onde pode-se determinar quais processos podem ser executados ou não;

1.45. Permitir bloqueio de rede da estação enquanto não for confirmado se a máquina possui antivírus instalado, se o mesmo se encontra atualizado e dentro da política de antivírus e de filtro de pacotes para estações;

1.46. Permitir criar regras de bloqueio/permissão utilizando protocolos ou aplicações;

1.47. Possuir gerenciamento centralizado;

1.48. Possuir integração com a mesma ferramenta de gerencia do antivírus;

1.49. Possibilitar a integração de políticas definidas pelo administrador com o usuário local;

1.50. Instalação automática em maquinas novas na rede, via software de gerencia;

1.51. Possuir tecnologia de detecção em nuvem, baseada em "fingerprint" de arquivos suspeitos;

1.52. Deverá possuir solução para estações de Trabalho 32 bits e 64 bits. (Antivírus, Antispyware, IPS e Proteção de Navegador) com as seguintes características:

1.52.1. Suporte a Windows XP, Windows Vista, Windows 7;

1.52.2. Suporte total a plataforma 64 bits;

1.52.3. Todas as funcionalidades deste item devem ser ativadas por agente único que facilita a instalação, a configuração e o gerenciamento. O agente deverá ser o mesmo agente do software de Antivírus;

1.52.4. Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções:

1.52.4.1. Limpar arquivos automaticamente;
1.52.4.2. Excluir arquivos Automaticamente; e
1.52.4.3. Negar Acesso aos Arquivos (quarentena).

1.52.5. Rastreamento manual com interface Windows, customizável, com opção de limpeza;

1.52.6. Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável;

1.52.7. Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo;

1.52.8. Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers, etc.;

1.52.9. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador;

1.52.10. Permitir atualização incremental da lista de definições de vírus;

1.52.11. Salvar automaticamente as listas de definições de vírus em local especificado na rede, após cada atualização bem-sucedida;

1.52.12. Programação de rastreamentos automáticos do sistema com as seguintes opções:

1.52.12.1. Escopo: Todos os drives locais, drives específicos, ou pastas específicas;

1.52.12.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

1.52.12.3. Frequência: Horária, diária, semanal, mensal; e

1.52.12.4. Exclusões: Pastas ou arquivos que não devem ser rastreados.

1.52.13. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

1.52.14. Gerar notificações de eventos de vírus através de alerta na rede;

1.52.15. Permitir a instalação em ambientes em Cluster Microsoft;

1.52.16. Permitir bloqueio de aplicações pelo nome do arquivo;

1.52.17. Possibilidade de reparar o registro do sistema após eliminação de epidemia;

1.52.18. Permitir bloqueio de portas;

1.52.19. Permitir criação de regras baseadas em processos de sistema;

1.52.20. Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia;

1.52.21. Possuir proteção contra estouro de buffer;

1.52.22. Capacidade de retomar atualizações de DAT's e de software do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinicio de todo o processo;

1.52.23. Detecção de cookies potencialmente indesejáveis no sistema;

1.52.24. O sistema de antispyware deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca DAT de definições de vírus e demais ameaças;

1.52.25. Possuir a capacidade de monitorar e bloquear as invasões, combinando proteção comportamental e a proteção por características com um firewall e um único produto;

1.52.26. O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus antispyware, antispam e controle de acesso à rede. Possibilitando uma única e simples interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum software adicional a console de gerenciamento para permitir o controle integrado;

1.52.27. Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP;

1.52.28. Deve possuir o recurso de blindagem, impedindo o comprometimento dos aplicativos e dos seus dados, além de evitar que um aplicativo seja usado para atacar outros aplicativos;

1.52.29. Possuir proteção, pronta para operação e contra vulnerabilidades desconhecidas, tais como buffer overflow e ataques de dia zero (zero-day attacks);

1.52.30. Possuir proteção contra BOTs;

1.52.31. Estar de acordo com as regulamentações GLBA, CA Breach Act 1386, Sarbanes-Oxley e HIPAA;

1.52.32. Capacidade de trabalhar no modo adaptativo se adaptando a novas aplicações instaladas na máquina;

1.52.33. Disponibilizar os seguintes relatórios na plataforma de gerencia: sumário de eventos de IPS por assinatura, por alvo, por endereço IP origem, os 10 principais nós atacados, as 10 principais assinaturas, sumário das aplicações bloqueadas e update de quarentena;

1.52.34. Permitir o bloqueio de ataques baseados em Web como: Directory Traversal attacks e Unicode attacks;

1.52.35. Interceptar tráfego e requisições de HTTP após decriptação e decodificação;

1.52.36. Permitir o bloqueio de aplicações e os processos que a aplicação interage;

1.52.37. Funcionar tanto no ambiente corporativo como em VPN;

1.52.38. Trabalhar no modo de quarentena permitindo a verificação pelo software de gerenciamento se o cliente está trabalhando com políticas antigas e versões desatualizadas, neste caso, o cliente é

bloqueado a uma área de quarentena, limitando a acesso a rede desta estação;

1.52.39. Capacidade de detectar e bloquear tentativas de invasão;

1.52.40. Possuir instalação "silenciosa";

1.52.41. Bloquear acessos indevidos que não estejam na tabela de políticas definidas pelo administrador;

1.52.42. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;

1.52.43. Permitir monitoração de *hooking* de aplicações onde pode-se determinar quais processos podem ser executados ou não;

1.52.44. Permitir bloqueio de rede da estação enquanto não for confirmado se a máquina possui antivírus instalado, se o mesmo se encontra atualizado e dentro da política de antivírus e de filtro de pacotes para estações;

1.52.45. Permitir criar regras de bloqueio/permissão utilizando protocolos ou aplicações;

1.52.46. Possuir gerenciamento centralizado;

1.52.47. Possuir integração com a mesma ferramenta de gerencia do antivírus;

1.52.48. Possibilitar a integração de políticas definidas pelo administrador com o usuário local;

1.52.49. Instalação automática em maquinas novas na rede, via *software* de gerencia;

1.52.50. Possuir tecnologia de detecção em nuvem, baseada em "*fingerprint*" de arquivos suspeitos;

1.52.51. Possuir ferramenta integrada para verificação de reputação de websites;

1.52.52. Possibilidade de configuração de bloqueio de acesso aos sites maliciosos pela console de gerenciamento;

1.52.53. Possibilidade de criar *blacklists* e *whitelists* de *urls* para estações pela console de gerenciamento;

1.53. Deverá possuir módulo para Gerenciamento da solução Antivírus – gerência centralizada de todos os módulos da suíte:

1.53.1. Suporte a instalação do servidor na plataforma Windows 2003 Server e Windows 2008 Server;

1.53.2. Suporte a instalação em cluster Microsoft;

1.53.3. Suportar o gerenciamento de até 250.000 máquinas a partir de um único servidor;

1.53.4. Permitir o gerenciamento do servidor através do protocolo TCP/IP e HTTP;

1.53.5. Permitir a instalação dos Módulos da Solução a partir de um único servidor;

1.53.6. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota;

1.53.7. Possuir agentes capazes de efetuar a comunicação direta com o banco de dados sem a necessidade de conexão com o servidor de gerenciamento;

1.53.8. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local;

1.53.9. Visualização das características básicas de hardware das máquinas;

1.53.10. Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local;

1.53.11. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede;

1.53.12. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;

1.53.13. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede;

1.53.14. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;

1.53.15. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente;

1.53.16. Permitir a criação de grupos virtuais através de "TAGs";

1.53.17. Permitir aplicar as "TAGs" nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, etc.;

1.53.18. Forçar a configuração determinada no servidor para os clientes. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente;

1.53.19. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS;

1.53.20. Forçar a instalação dos Módulos da Solução nos clientes. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido;

1.53.21. Customização dos relatórios gráficos gerados;

1.53.22. Exportação dos relatórios para os seguintes formatos: HTML, CSV e PDF;

1.53.23. Geração de relatórios que contenham as seguintes informações:

1.53.23.1. Máquinas com a lista de definições de vírus desatualizada;

1.53.23.2. Qual a versão do software instalado em cada máquina;

1.53.23.3. Os vírus que mais foram detectados;

1.53.23.4. As máquinas que mais sofreram infecções em um determinado período de tempo; e

1.53.23.5. Os usuários que mais sofreram infecções em um determinado período de tempo.

1.53.24. Gerenciamento de todos os módulos da suíte;

1.53.25. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local e dial-up;

1.53.26. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;

1.53.27. Ter a capacidade de gerar registros/logs para auditoria;

1.53.28. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento;

1.53.29. A solução de gerenciamento deve permitir acesso a sua console via web;

1.53.30. Implementação de Dashboard com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida;

1.53.31. Deverá possuir antivírus para Servidores de Groupware;

1.53.32. Servidores Microsoft Exchange Server:

1.53.32.1. Instalação nas plataformas Windows 2000, Windows 2003;

1.53.32.2. Suporte a plataforma windows 2000, 2003 e 2007; e

1.53.32.3. Rastreamento em tempo real, para arquivos anexados a mensagens do Exchange, antes de entregar a mensagem na caixa postal do(s) destinatário(s), com as seguintes opções:

1.53.32.3.1. Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);

1.53.32.3.2. Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s); e

1.53.32.3.3. Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s).

1.53.32.4. Rastreamento manual às pastas do Exchange, com opção de limpeza;

1.53.32.5. Programação de rastreamentos automáticos do Exchange com as seguintes opções:

1.53.32.5.1. Escopo: Todas as pastas locais, ou pastas específicas;

1.53.32.5.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena); e

1.53.32.5.3. Frequência: Horária, diária, semanal, mensal.

1.53.32.6. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

1.53.32.7. Gerar notificações de eventos de vírus através de mensagens do Exchange para quem enviou e quem recebeu a mensagem, e para um Administrador (usuário opcional);

1.53.32.8. Identificação de remetente e destinatário das mensagens;

1.53.32.9. Permitir bloqueios baseados nos seguintes critérios:

1.53.32.9.1. Tipo de arquivo;

1.53.32.9.2. Nome do arquivo;

1.53.32.9.3. Tamanho do arquivo;

1.53.32.10. Permitir a instalação em ambientes em Cluster Microsoft; e

1.53.32.11. Capacidade de filtragem de conteúdo por categorias como: Sexo, Drogas, etc.

1.53.33. Servidores Lotus Domino:

1.53.33.1. Instalação nas plataformas Windows NT Server 4.0, Windows 2000, Windows 2003 e AIX;

1.53.33.2. Instalação no Servidor Domino na forma de "Task";

1.53.33.3. Rastreamento em tempo real, para arquivos anexados a mensagens do Domino, antes de entregar a mensagem na caixa postal do(s) destinatário(s), com as seguintes opções:

1.53.33.3.1. Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);

1.53.33.3.2. Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s); e

1.53.33.3.3. Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s).

1.53.33.4. Rastreamento manual às bases do Domino, com opção de limpeza;

1.53.33.5. Programação de rastreamentos automáticos do Domino com as seguintes opções:

1.53.33.5.1. Escopo: Todas as bases locais, ou bases específicas;

1.53.33.5.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena); e

1.53.33.5.3. Frequência: Horária, diária, semanal, mensal.

1.53.33.6. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

1.53.33.7. Gerar notificações de eventos de vírus através de mensagem do Notes para quem enviou e quem recebeu a mensagem, e para um Administrador (usuário opcional);

1.53.33.8. Permitir bloqueios baseados nos seguintes critérios:

1.53.33.8.1. Tipo de arquivo;

1.53.33.8.2. Nome do arquivo; e

1.53.33.8.3. Tamanho do arquivo.

1.53.33.9. Permitir a instalação em ambientes de Cluster;

1.53.34. A console de gerenciamento deve suportar a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;

1.53.35. A console de gerenciamento deve suportar criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente;

1.53.36. A console de gerenciamento deve permitir a criação de grupos virtuais através de "TAGs";

1.53.37. A console de gerenciamento deve permitir aplicar as "TAGs" nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, etc.;

1.54. A solução deverá ter garantia de atualização por um período de 36 (trinta e seis) meses;

1.55. O fornecedor da solução deverá prestar suporte técnico on-site em até 04 horas úteis após a abertura do chamado, durante a vigência do contrato;

1.56. O fornecedor da solução deverá prestar suporte via e-mail e telefone 24 x 7 durante a vigência do contrato;

1.57. O fornecedor da solução realizará treinamento para utilização do produto, a ser ministrado fora das dependências da EPL, e na cidade de Brasília-DF, para no mínimo 08 (oito) técnicos indicados pela EPL. Subordinadas, com 12 (doze) horas de duração em data e horários estabelecidos pela EPL;

1.58. A EPL, ao final do treinamento, passará uma pesquisa de satisfação com os participantes para verificar se os objetivos foram atingidos. Caso o índice mínimo não seja atingido o fornecedor repetirá o treinamento;

1.59. O fornecedor deverá providenciar atualização automática do produto mantendo-o sempre em sua última versão com todas as suas características, durante a vigência do contrato;

1.60. O fornecedor deverá providenciar a instalação e configuração da solução por técnico(s) certificado(s) pelo fabricante da solução;

1.61. O fornecedor deverá comprovar que o(s) técnico(s) possui(em) habilitação para executar os serviços de instalação, configuração e manutenção on-site, apresentando certificado técnico emitido pelo fabricante da solução, por ocasião da execução do serviço na EPL;

1.62. O fornecedor deverá apresentar declaração do fabricante da solução ou do representante por esta indicado, de que a revenda está apta a prestar os serviços ofertados, com técnicos treinados e certificados bem como solidariedade do fabricante na implantação da solução proposta; e

1.63. O fornecedor deverá apresentar no mínimo 01 (hum) atestado de capacidade técnica de fornecimento da solução ofertada de pessoa de direito público ou privado.

ANEXO "B"

NOTA DE EMPENHO

ANEXO "C"

PROPOSTA DA CONTRATADA

ANEXO "D"

ATA DE REGISTRO DE PREÇOS