CONTRATO ADMINISTRATIVO N.º 19/2017 CELEBRADO ENTRE A EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A – EPL E A EMPRESA ALTAS NETWORKS & TELECOM LTDA PARA CONTRATAÇÃO DE SOLUÇÃO DE ALTA DISPONIBILIDADE DE *NEXT GENERATION FIREWALL – NGFW* COM GERENCIAMENTO CENTRALIZADO E INTEGRADO, ATUALIZAÇÕES DE PROTEÇÃO E SUPORTE TÉCNICO, 24X7, PELO PRAZO DE 36 MESES, INCLUINDO SERVIÇOS DE INSTALAÇÃO E TREINAMENTO.

CONTRATANTE: EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A. - EPL, inscrita no CNPJ (MF) n.º 15.763.423/0001-30, e Inscrição Estadual GDF nº 07.622.898/001-15, com sede no Setor Comercial Sul, Quadra 9, Lote C, Complexo Parque Cidade Corporate, Torre C – 7º e 8º andares, em Brasília/DF, CEP 70308-200, representada pelo Diretor de Gestão, Senhor **MAURÍCIO PEREIRA MALTA**, brasileiro, casado, portador da RG nº 1243998-SSP/ES e do CPF n.º 507.460.655-15, nomeado pela Ata da 8ª Reunião Extraordinária do Conselho de Administração de 22 de dezembro de 2016, e pelo Diretor Presidente, Senhor **JOSE CARLOS MEDAGLIA FILHO**, brasileiro, casado, engenheiro civil, portador da Carteira de identidade RG nº 2.916.693 SSP/DF e inscrito no CPF/MF sob o nº 388.908.520-20, domiciliado em Brasília – DF, nomeado pela Ata da 7ª Reunião Extraordinária do Conselho de Administração de 2 de agosto de 2016.

CONTRATADA: ALTAS NETWORKS & TELECOM LTDA, inscrita no CNPJ sob o nº 05.407.609/0001-01, Inscrição Estadual MG nº 062.212.833-0032, com sede na Rua Juruá nº 46, 7º andar, salas 704 a 708 – Bairro da Graça, Belo Horizonte, MG, CEP: 31.140-020, neste ato representado pelo Senhor **ALMIR FRANZ DE LIMA,** brasileiro, casado, portador da Cédula de Identidade nº MG -2.880.975, SSP/MG, inscrito no CPF(MF) sob o nº 591.914.736-91, de acordo com a representação legal que lhe é outorgada por Contrato Social.

Os CONTRATANTES têm entre si justo e avençado, e celebram o presente contrato, tendo

em vista o que consta no Processo nº 50840.000238/2017-78 e em observância às disposições da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 7.892, de 23 de janeiro de 2013, do Decreto nº 2.271, de 7 de julho de 1997, da Instrução Normativa SLTI/MP nº 04/2014 e suas alterações, da Instrução Normativa SLTI/MPOG n° 02, de 2008 e subsidiariamente na Lei 8.666, de 21 de junho de 1993, e demais normas correlatas, decorrente da adesão à Ata de Registro de Preços oriunda do Pregão nº 100/2016 da Fundação Universidade Federal de São João Del-Rei - UFSJ, UASG: 154069, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. CONTRATAÇÃO DE SOLUÇÃO DE ALTA DISPONIBILIDADE DE *NEXT GENERATION FIREWALL – NGFW* COM GERENCIAMENTO CENTRALIZADO E INTEGRADO, ATUALIZAÇÕES DE PROTEÇÃO E SUPORTE TÉCNICO, 24X7, PELO PRAZO DE 3(MESES, INCLUINDO SERVIÇOS DE INSTALAÇÃO E TREINAMENTO, que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital do Pregão Eletrônico nº 100/2016 da Fundação Universidade Federal de São João Del-Rei, UASG: 154069.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão Eletrônico nº 100/2016 da Fundação Universidade Federal de São João Del-Rei, UASG: 154069, identificado no preâmbulo e à proposta da contratada, independentemente de transcrição.

1.3. Este Contrato vincula-se ao Termo de Referência constante das fls. 131/150 do Processo 50840.000238/2017-78.

1.4. Objeto da contratação:

Itens do Processo	Descrição	Unidade	Quantitativo a ser contratado
4	Firewall	unidade	2
9	Software de relatórios	licença	1

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Contrato é de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, tendo eficácia após publicado o respectivo extrato na Imprensa Oficial, improrrogáveis.

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor da contratação é de **R$ 294.000,00 (duzentos e noventa e quatro mil reais),** conforme tabela abaixo:

ITEM	DESCRIÇÃO	QUANT.	UND.	VALOR UNITÁRIO	VALOR TOTAL
4	FIREWALL	2	UNIDADE	125.000,00	250.000,00
9	SOFTWARE	1	Licença	44.000,00	44.000,00
Total					**R$ 294.000,00**

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2017, na classificação abaixo:

Gestão/Unidade: 395001
Fonte: 100
Elemento de Despesa: 4490
PI: 26.121.2101.20UA.0001

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O pagamento será realizado no prazo máximo de 15 (quinze) dias úteis, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agencia e conta indicado pela Contratada.

5.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

5.3. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 03 (três) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

5.4. O pagamento somente será autorizado depois de efetuado o "atesto" pela fiscalização do contrato, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados.

5.5. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

5.6. Nos termos do artigo 36, § 6°, da Instrução Normativa SLTI/MPOG n° 02, de 2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

5.6.1. não produziu os resultados acordados;

5.6.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

5.6.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

5.7. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

5.8. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

5.9. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

5.10. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

5.11. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

5.12. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao

ALTAS NETWORKS

5.13. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante, não será rescindido o contrato em execução com a contratada inadimplente no SICAF.

5.14. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

5.14.1. A Contratada regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

5.15. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

Onde:

EM = Encargos Moratórios.

VP = Valor da parcela a ser paga.

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.

I = índice de compensação financeira = 0,0001644, assim apurado:

$$\frac{I = (TX)}{365} \qquad \frac{I = (6/100)}{365} \qquad I = 0{,}0001644$$

TX = Percentual da taxa anual = 6%

6. CLÁUSULA SEXTA – INEXISTÊNCIA DE REAJUSTE

6.1. O preço é fixo e irreajustável.

7. CLÁUSULA SÉTIMA - DA GARANTIA TÉCNICA

7.1. O objeto deste contrato deverá contar com a Garantia Técnica, nos termos do item 5.10 do Termo de Referência constante das fls. 131/150 do Processo 50840.000238/2017-78.

8. CLÁUSULA OITAVA – REGIME DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. O regime de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de

Referência, anexo do Edital do Pregão Eletrônico nº 100/2016 da Fundação Universidade Federal de São João Del-Rei, UASG: 154069.

8.2. O objeto desta contratação deverá ser executado em exata observância no Termo de Referência constante das fls. 131/150 do Processo 50840.000238/2017-78.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. São obrigações da CONTRATANTE:

a) receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

b) verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

c) comunicar à contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

d) acompanhar e fiscalizar o cumprimento das obrigações da contratada, através de comissão/servidor especialmente designado; e

e) efetuar o pagamento à contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital da licitação e seus anexos;

9.2. A Administração não responderá por quaisquer compromissos assumidos pela contratada com terceiros, ainda que vinculados à execução do Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos ou subordinados.

9.3. São Obrigações da CONTRATADA

9.4. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

a) efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

b) O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada;

ALTAS NETWORKS

c) responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

d) substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

e) comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

f) manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação; e

g) indicar preposto para representá-la durante a execução do contrato;

9.5. A contratada deverá prestar serviços de manutenção e suporte técnico a todos os produtos contratados, no local de instalação da solução, sem ônus para a EPL, durante os sete dias da semana, incluindo finais de semana e feriados, 24 (vinte e quatro) horas por dia (7x24), conforme condições e prazos previstos do Edital da licitação e neste documento.

10. CLÁUSULA DÉCIMA – SANÇÕES ADMINISTRATIVAS.

10.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

a) inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
b) ensejar o retardamento da execução do objeto;
c) fraudar na execução do contrato;
d) comportar-se de modo inidôneo;
e) cometer fraude fiscal;
f) não mantiver a proposta.

10.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

b) multa moratória de 0,1% (um décimo por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 2% (dois por centos);

c) multa compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

d) em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

e) suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 anos.

f) declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base na alínea anterior.

10.3. A sanção estabelecida na alínea "f", subitem 11.2 é de competência exclusiva do Ministro de Estado, facultada a defesa da CONTRATADA no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

10.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

a) tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

10.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

10.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

10.7. As penalidades serão obrigatoriamente registradas no SICAF.

ALTAS NETWORKS

11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas neste Contrato.

11.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

11.4. O termo de rescisão, sempre que possível, será precedido:

11.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES

12.1. É vedado à CONTRATADA:

12.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

12.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessária, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.2.1. É vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666, de 1993.

13.3. As supressões resultantes de acordo celebrados entre as contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.4. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da EPL quanto à continuidade do contrato.

14. CLÁUSULA DÉCIMA QUARTA – DA SUBCONTRATAÇÃO

14.1. Não será admitida a subcontratação do objeto contratado

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1 Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

17.1. O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Seção Judiciária de. Brasília-DF - Justiça Federal.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

Brasília, 26 de dezembro de 2017.

JOSE CARLOS MEDAGLIA FILHO
DIRETOR PRESIDENTE

MAURÍCIO PEREIRA MALTA
DIRETOR DE GESTÃO

ALMIR FRANZ DE LIMA
CONTRATADA

TESTEMUNHAS:

NOME:
CPF:
RG n.º:

Andrea Abrão Paes Leme
Mat. SIAPE nº 1990146
EPL

NOME:
CPF:
RG n.º:

Eduardo Solano Spim
Mat. SIAPE Nº: 2028629
EPL

1. DEFINIÇÃO E ESPECIFICAÇÕES TÉCNICAS MÍNIMAS NECESSÁRIAS

1.1. Appliance de firewall

1.1.1. Características de hardware e performance:

- *Throughput* de, no mínimo, 24 Gbps com a funcionalidade de *firewall* habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
- Suporte a, no mínimo, 5 milhões de conexões simultâneas;
- Suporte a, no mínimo, 270 mil novas conexões por segundo;
- Throughput de, no mínimo, 16 Gbps de VPN IPSec;
- Estar licenciado para ou suportar sem o uso de licença, 2 mil túneis de VPN IPSEC Site-to-Site simultâneos;
- Estar licenciado para ou suportar sem o uso de licença, 10 mil túneis de clientes VPN IPSEC simultâneos;
- Throughput de, no mínimo, 2.2 Gbps de VPN SSL;
- Suporte a, no mínimo, 5 mil clientes de VPN SSL simultâneos;
- Suportar no mínimo 4 Gbps de throughput de IPS;
- Suportar no mínimo 3.5 Gbps de throughput de Inspeção SSL;
- Throughput de, no mínimo, 2.4 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- Possuir ao menos 16 interfaces 1Gbps;
- Possuir ao menos 2 interfaces 10Gbps;
- Disco de, no mínimo, 120 GBytes para armazenamento de informações locais
- Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
- Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

1.1.2. Requisitos mínimos de funcionalidade:

- A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall-NGFW, e console de gerência e monitoração;
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- O software deverá ser fornecido em sua versão mais atualizada;
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede;
- Os dispositivos de proteção de rede devem possuir suporte a 1024 VLAN Tags 802.1q;
- Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP;
- Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- Deve suportar NAT dinâmico (Many-to-1);
- Deve suportar NAT dinâmico (Many-to-Many);
- Deve suportar NAT estático (1-to-1);
- Deve suportar NAT estático (Many-to-Many);
- Deve suportar NAT estático bidirecional 1-to-1;
- Deve suportar Tradução de porta (PAT);
- Deve suportar NAT de Origem;

ALTAS NETWORKS LICITAÇÃO

- Deve suportar NAT de Destino;
- Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- Deve suportar NAT64 e NAT46;
- Deve implementar o protocolo ECMP;
- Deve implementar balanceamento de link por hash do IP de origem;
- Deve implementar balanceamento de link por hash do IP de origem e destino;
- Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
- Deve suportar o balanceamento de, no mínimo, quatro links;
- Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- Enviar log para sistemas de monitoração externos, simultaneamente;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- Proteção anti-spoofing;
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- Suportar OSPF graceful restart;
- Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
- A configuração em alta disponibilidade deve sincronizar: Sessões;
- A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
- A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
- A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
- O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- A utilização dos dispositivos em alta disponibilidade não deve impor limitações quanto à utilização de sistemas virtuais (contextos);
- Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
- O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
- Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolação das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
- As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, o licenciamento do dispositivo de segurança não pode ter nenhuma relação com sua configuração de rede como, mas não limitado a, configuração de interfaces, endereços

lógicos, etc , podendo ser utilizado por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *software* com o fabricante.

- Deverá suportar controles por zona de segurança;
- Controles de políticas por porta e protocolo;
- Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
- Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
- Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- Controle de inspeção e de-criptografia de SSH por política;
- Suporte a objetos e regras IPV6;
- Suporte a objetos e regras multicast;
- Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

1.1.3. **Controle de aplicações:**

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software,

protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

- Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over, http, gotomeeting, webex, evernote, google-docs, etc;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
- Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;
- Identificar o uso de táticas evasivas via comunicações criptografadas;
- Atualizar a base de assinaturas de aplicações automaticamente;
- Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

ALTA NETWORKS LICITAÇÃO

- Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MSSQL, IMAP, DNS, LDAP, RTSP e SSL;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook, Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon3, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Categoria da aplicação

- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Aplicações que usem técnicas evasivas, utilizadas por malwares como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos, etc.

1.1.4. **Prevenção de ameaças:**

- Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
- As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura;
- Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve incluir proteção contra ataques de negação de serviços;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;

ALTAS NETWORKS LICITAÇÃO

- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- Detectar e bloquear a origem de portscans;
- Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- Possuir assinaturas para bloqueio de ataques de buffer overflow;
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e antispyware, permitindo a criação de exceções com granularidade nas configurações;
- Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Identificar e bloquear comunicação com botnets;
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação;
- Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

- Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- Proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

1.1.5. **Filtro de URL:**

- Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- Possuir pelo menos 60 categorias de URLs;
- Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- Permitir a customização de página de bloqueio;
- Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).

1.1.6. **Identificação de usuários:**

- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
- Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
- Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

1.1.7. **QoS e Traffic Shaping:**

- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
- Suportar a criação de políticas de QoS e Traffic Shaping por porta;
- O QoS deve possibilitar a definição de classes por Banda Garantida;
- O QoS deve possibilitar a definição de classes por Banda Máxima;
- O QoS deve possibilitar a definição de classes por Fila de Prioridade
- Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

1.1.8. **Filtro de dados:**

- Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1.1.9. **Geo Localização:**

- Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

1.1.10. **VPN:**

- Suportar VPN Site-to-Site e Cliente-To-Site;
- Suportar IPSec VPN;
- Suportar SSL VPN;
- A VPN IPSEc deve suportar 3DES;
- A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN;
- IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

- A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- Atribuição de DNS nos clientes remotos de VPN;
- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- Suportar leitura e verificação de CRL (certificate revocation list);
- Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SCCM, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;
- Deverá manter uma conexão segura com o portal durante a sessão;
- O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows XP (32 bit), Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

1.1.11. **Condições operacionais:**

- Alimentação / tensão de 100-240 VAC;
- Possuir conector para fonte de alimentação externa redundante;
- Alimentação / frequência de 50/60 Hz;
- Temperatura - faixa de operação de 0° a 40° C.

1.2. Software de relatórios

1.2.1. Características gerais

- Deve ser do mesmo fabricante dos itens de firewall, a fim de garantir compatibilidade;
- Deve estar licenciado para coletar logs e gerar relatório de múltiplos firewalls;
- Possuir capacidade receber ao menos 5GBytes de logs diários;
- Caso a solução de coleta de logs e relatórios seja ofertada em appliance físico deverá possuir ao menos 4 interfaces de 1Gbps RJ-45, 16GB de memória RAM, um processador octacore e ao menos 3 TB de armazenamento configurados em RAID 1;
- Caso a solução de gerenciamento seja ofertada em appliance virtual deverá ser compatível com ambiente VMware ESXi 5.5, estar licenciado para pelo menos 3 TB de espaço em disco e não deve possuir limite para suporte a expansão de memória RAM caso virtual;

1.2.2. Funcionalidades gerais:

- Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução;
- Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH);
- Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração;
- Suportar SNMP versão 2 e versão 3 na solução de relatórios;
- Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
- Deve permitir a criação de administradores que acessem à todas as instâncias de virtualização da solução de relatórios;
- Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;
- Autenticação integrada a servidor Radius;
- Geração de relatórios com mapas geográficos ou modo tabela gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- Autenticação integrada ao Microsoft Active Directory;

- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha do mesmo;
- Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado;
- Possuir mecanismo para que logs antigos sejam removidos automaticamente;
- Permitir a importação e exportação de relatórios;
- Deve ser possível exportar os logs em CSV;
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar;
- A solução deve possuir relatórios pré-definidos;
- Possuir envio automático de logs para um servidor FTP externo a solução;
- Possibilitar a duplicação de relatórios existentes e edita-los Possuir a capacidade de personalização de capas para os relatórios;
- Possibilitar a duplicação de gráficos existentes de relatórios;
- Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log;
- Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;
- Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios;
- Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime;
- Dever ser possível fazer download dos arquivos de logs recebidos;
- Deve possuir agendamento para gerar e enviar automaticamente relatórios;
- Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades;
- Permitir o envio de maneira automática de relatórios por email;
- Deve permitir a escolha do email a ser enviado para cada relatório escolhido;
- Permitir programar a geração de relatórios, conforme calendário definido pelo administrador;

- Deve ser possível definir filtros nos relatórios;
- Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;
- Permitir que relatórios criado sejam no idioma Português;
- Gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros;
- Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
- Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;
- Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros;
- Deve possuir a informação de Indicador de Compromisso (IoC);
- Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o objetivo de detectar problemas de performance de sistema de acordo com o relatório criado;
- Permitir que a solução busque log arquivados de outros dispositivos da mesma solução;
- Deve possuir relatório de PCI DSS Compliance;
- Deve ser possível definir o espaço que cada instância de virtualização poderá utilizar para armazenamento de logs;
- A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes;
- Deve suportar duplo fator de autenticação (token) para os administradores do sistema de relatórios;
- Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo e caracteres a usar;
- Deve permitir ver em tempo real os logs recebidos.

Empresa de Planejamento e Logística

Empresa de Planejamento e Logística Fls. 224 Rubrica EPL

ANEXO B

TERMO DE COMPROMISSO DA MANUTENÇÃO DE SIGILO

A Empresa **ALTAS NETWORKS & TELECOM LTDA**, inscrita no CNPJ sob o n.º 05.407.609/0001-01, sediada na Rua Juruá nº 46, 7º andar, salas 704 a 708 – Bairro da Graça, Belo Horizonte, MG, CEP: 31.140-020, por intermédio de seu representante legal, Senhor **ALMIR FRANZ DE LIMA,** brasileiro, casado, portador da Cédula de Identidade n.º MG -2.880.975, expedida pela(o) SSP/MG e CPF n.º 591.914.736-91, **DECLARA** para fins de celebração da contratação com a Empresa de Planejamento e Logística – EPL, CNPJ nº 15.763.423/0001-30, que se compromete a **manter em sigilo**, ou seja, não revelar ou divulgar as informações da EPL, ou de seus empregados, obtidas em razão da execução contratual, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de seu conhecimento. A empresa está ciente que, caso tenha acesso à base de informações da EPL inserida no sistema, ela deverá preservar tais informação e, em nenhuma hipótese, divulgá-las sem autorização formal da EPL. A Empresa declara, ainda, que dará ciência aos seus empregados sobre a obrigação de manter sigilo sobre as informações obtidas em razão da execução contratual em pauta.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar a EPL de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, danos, perdas, custas e despesas que porventura venha sofrer como resultado da violação do disposto neste instrumento.

ALMIR FRANZ DE LIMA
CONTRATADA
RG: MG -2.880.975 – SSP/MG
CPF: 591.914.736-91

Empresa de Planejamento e Logística

ANEXO E

TERMO DE RECEBIMENTO DEFINITIVO

Processo nº:	**Contrato nº:**
Objeto:	**Vigência:**
Contratada:	**CNPJ:**
Licenças:	
Valor:	
Data prevista para entrega:	
Data da efetiva entrega:	

Por este instrumento, atesto, para fins de cumprimento do disposto no art. 34, inciso VIII, da Instrução Normativa SLTI/MP nº 4/2014, a Aquisição de uma solução de descoberta de dados (Data Discovery), com licenças de software de uso perpétuo, em conjunto com os serviços de instalação e configuração, suporte técnico e atualização de versão, treinamento (capacitação técnica) e de suporte especializado, conforme Lista de Verificação anexa.

Os fornecimentos das licenças foram adquiridos de forma satisfatória, razão pela qual lavramos este TERMO DE RECEBIMENTO DEFINITIVO, para os fins legais e para efeitos de pagamento.

De acordo,

Brasília, de de 2017.

Fiscal Requisitante	**Gestor**
Preposto da Contratada	
Assinatura **RG Nº**	

Empresa de Planejamento e Logística

Empresa de Planejamento e Logística
Fls. 226
Rubrica
EPL

ANEXO F
LISTA DE VERIFICAÇÃO

Contrato:	**Mês de Referência:**	**Período Verificado:**
RECEBIMENTO DEFINITIVO		
Item	**Aceite**	
Disponibilização de acesso da EPL ao Sistema		
Realização da Instalação		
Disponibilização do suporte técnico do Sistema à EPL.		
Conformidade do Atendimento do Suporte Técnico		
Funcionamento e disponibilidade plena e diária do Sistema no mês de faturamento		
Atendimento das necessidades da contabilidade pela solução		
Cumprimento de Prazos		
Cumprimento das obrigações contratuais		
Verificação da Regularidade Fiscal, Trabalhista e Previdenciária da contratada		
Data da Verificação:	**Data da Verificação:**	
Assinatura **Fiscal Requisitante** **Assinatura** **Gestor**		

3) No campo "Aceite", marcar "atende", "não atende", ou "conforme relatório anexo" (detalhar ajustes de pagamento, desconformidades, dentre outros em relatório anexado à lista).

4) A lista de verificação é instrumento da Equipe de Fiscalização e poderá ser alterada conforme suas necessidades ao longo da vigência da contratação.

Empresa de Planejamento e Logística

ANEXO G

MODELO DE ORDEM DE SERVIÇO

A Empresa de Planejamento e Logística – EPL, por meio do servidor (*nome*), matrícula SIAPE (*número*), e em face do Contrato em epígrafe, requer à Empresa (*nome*), CNPJ (*número*), endereço (*indicar*), telefone (*indicar*), e-mail (*indicar*), a disponibilização do Software, conforme abaixo indicado:

Software a ser fornecido: (*indicar*)

Quantidades de licenças : (*indicar*)

Prazo: (*indicar*)

Endereço: (*indicar*)

_____

Nome/carimbo e Assinatura do Servidor

Recebi, em ___/___/____, a presente Ordem de Serviço, obrigando-me desde já a realizar o serviço dela constante, no prazo e valor acima indicado.

_____

Nome e Assinatura do Responsável Legal pela Contratada

RG e CPF

Espécie: Convênio Nº 854992/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Querência, CNPJ 37.465.002/0001-66. Recuperação de estradas vicinais padrão alimentadoras no Projeto de Assentamento Pingo D'água. Localização município de Querência, estado de Mato Grosso - MT. Valor Total: R$ 721.022,45. Valor de Contra-Partida: R$ 21.022,45. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800606. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF 161.458.601-20, Convenente: Fernando Gorgem, CPF 605.473.759-72.

Espécie: Convênio Nº 853257/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Rondonópolis, CNPJ 03.347.101/0001-21. Implantação de Rede de Distribuição de Água no Projeto de Assentamento PA Carimã. Localização município de Rondonópolis, estado de Mato Grosso - MT. Valor Total: R$ 1.050.000,00. Valor de Contra- Partida: R$ 50.000,00. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800572. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF: 161.458.601-20, Convenente: JOSÉ CARLOS DO PÁTIO, CPF: 716.086.611-87.

Espécie: Convênio Nº 855661/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Salto do Céu, CNPJ 15.024.011/0001-89. Recuperação de estradas vicinais no padrão alimentadora no Projeto de Assentamento Santa Cecília. Localização município de Salto do Céu, estado de Mato Grosso - MT. Valor Total: R$ 401.000,00. Valor de Contra-Partida: R$ 1.000,00. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800632. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF 161.458.601-20, Convenente: Wemerson Asão Prata, CPF 809.673.611-68.

Espécie: Convênio Nº 855916/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Sinop, CNPJ 02.287.538/0001-54. Recuperação de estradas vicinais no padrão alimentadora no Projeto de Assentamento Wesley Manoel dos Santos. Localização município de Sinop, estado de Mato Grosso - MT. Valor Total: R$ 2.000.000,00. Valor de Contra-Partida: R$ 100.000,00. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800610. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF 161.458.601-20, Convenente: Rosana Tereza Martinelli, CPF 325.760.051-87 .

Espécie: Convênio Nº 861589/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Sorriso, CNPJ 03.239.076/0001-62. Recuperação de estradas vicinais no padrão alimentadora no Projeto de Assentamento Santa Rosa. Localização município de Sorriso, estado de Mato Grosso - MT. Valor Total: R$ 540.000,00. Valor de Contra-Partida: R$ 40.000,00. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800674. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF 161.458.601-20, Convenente: Ari Genézio Lafin, CPF 411.319.161-15.

Espécie: Convênio Nº 856010/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Novo São Joaquim, CNPJ 03.238.581/0001-92. Recuperação de estradas vicinais no padrão alimentadora no Projeto de Assentamento Tamboril. Localização município de São Joaquim, estado de Mato Grosso - MT. Valor Total: R$ 1.010.000,00. Valor de Contra-Partida: R$ 10.000,00. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800622. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF 161.458.601-20, Convenente: Antônio Augusto Jordão, CPF 724.681.908-82.

Espécie: Convênio Nº 854844/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Vila Bela da Santíssima Trindade, CNPJ 03.214.160/0001-21. Recuperação de estradas vicinais no padrão alimentadora no Projeto de Assentamento Ritinha. Localização município de Vila Bela da Santíssima Trindade, estado de Mato Grosso - MT. Valor Total: R$ 309.000,00. Valor de Contra-Partida: R$ 9.000,00. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800618. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF 161.458.601-20, Convenente: Wagner Vicente da Silveira, CPF 125.443.291-49.

Espécie: Convênio Nº 861597/2017. Convenentes: Concedente: Instit. Nac. de Colonização e Reforma Agrária. Unidade Gestora: 373073, Gestão 37201. Convenente: Prefeitura Municipal de Vila Rica, CNPJ 03.238.862/0001-45. Recuperação de estradas vicinais no padrão alimentadora no Projeto de Assentamento PA IPÊ. Localização município de Vila Rica, estado de Mato Grosso - MT. Valor Total: R$ 303.000,00. Valor de Contra- Partida: R$ 3.000,00. Crédito Orçamentário: PTRES 139859. Fonte Recurso 0100000000 ND 4440-41/19. Num. Empenho 2017NE800678. Vigência: 29/12/2017 a 30/09/2018. Data de Assinatura: 29/12/2017. Signatários: Concedente: João Bosco de Moraes CPF: 161.458 601-20, Convenente: ABMAEL BORGES DA SILVEIRA, CPF: 328.086.072-72.

SUPERINTENDÊNCIA REGIONAL EM MINAS GERAIS

EXTRATOS DE CONVÊNIOS

Espécie: Convênio Nº 857191/2017, Nº Processo: 54000035122201701, Concedente: INSTIT. NAC. DE COLONIZACAO E REFORMA AGRARIA, Convenente: MUNICIPIO DE TUMIRITINGA CNPJ nº 21078563000172, Objeto: RECUPERAÇÃO DE ESTRADAS VICINAIS, Valor Total: R$ 251.000,00, Valor de Contrapartida: R$ 1.000,00, Valor a ser transferido ou descentralizado por exercício: 2018 - R$ 250.000,00, Crédito Orçamentário: Num Empenho: 2017NE800534, Valor: R$ 250.000,00, PTRES: 137063, Fonte Recurso: 0176370002, ND: 44404123, Vigência: 10/01/2018 a 11/12/2019, Data de Assinatura: 30/12/2017, Signatários: Concedente: ROBSON DE OLIVEIRA FONZAR CPF nº 930.997.461-34, Convenente: JOSE PAULO BRETAS CABRAL CPF nº 427.312.246-49.

Espécie: Convênio Nº 862517/2017, Nº Processo: 54000035129201714, Concedente: INSTIT. NAC. DE COLONIZACAO E REFORMA AGRARIA, Convenente: MUNICIPIO DE BONFINOPOLIS DE MINAS CNPJ nº 18125138000182, Objeto: RECUPERAÇÃO DE ESTRADAS VICINAIS COM CONSTRUÇÃO DE PONTES DE CONCRETO, Valor Total: R$ 252.500,00, Valor de Contrapartida: R$ 2.500,00, Valor a ser transferido ou descentralizado por exercício: 2018 - R$ 250.000,00, Crédito Orçamentário: Num Empenho: 2017NE800584, Valor: R$ 252.500,00, PTRES: 137063, Fonte Recurso: 0176370002, ND: 44404123, Vigência: 10/01/2018 a 11/12/2019, Data de Assinatura: 29/12/2017, Signatários: Concedente: ROBSON DE OLIVEIRA FONZAR CPF nº 930.997.461-34, Convenente: LUIZ CARLOS DA SILVA CPF nº 144.764.876-53.

SUPERINTENDÊNCIA REGIONAL NO RIO GRANDE DO SUL

AVISO DE LICITAÇÃO PREGÃO ELETRÔNICO Nº 1/2018 - UASG 373072

Nº Processo: 54000005164201890 . Objeto: Pregão Eletrônico - Contratação de pessoa jurídica para prestação de serviços de serviços de limpeza, higienização e conservação, com fornecimento de mão-de-obra, material de consumo, utensílios e equipamentos necessários), com jornada de trabalho de 44 hs semanais de segunda a sexta-feira, na forma de execução indireta, no regime de empreitada para atender as necessidades da Superintendência Regional do Rio Grande do Sul INCRA, Av. Loureiro da Silva, 515, Porto Alegre/RS, e para a Garagem da Superintendência, Sito mesmo logradouro, n.º 300 Total de Itens Licitados: 00001. Edital: 19/01/2018 de 09h00 às 12h00 e de 13h30 às 17h00. Endereço: Av.loureiro da Silva, 515 - 2.andar Centro - PORTO ALEGRE - RS ou www.comprasgovernamentais.gov.br/edital/373072-05-1-2018. Entrega das Propostas: a partir de 19/01/2018 às 09h00 no site www.comprasnet.gov.br. Abertura das Propostas: 31/01/2018 às 10h00 no site www.comprasnet.gov.br.

DIONISIO WESCHENFELDER
Chefe de Serv. de Adm. e Serv. Gerais

(SIDEC - 18/01/2018) 373072-37201-2017NE800097

SECRETARIA ESPECIAL DE AGRICULTURA FAMILIAR E DO DESENVOLVIMENTO AGRÁRIO

EXTRATO DE TERMO ADITIVO Nº 6/2018 - UASG 490002

Número do Contrato: 39/2015. Nº Processo: 55000001629201553 DISPENSA Nº 64/2015. Contratante: MINISTERIO DO DESENVOLVIMENTO -AGRARIO. CNPJ Contratado: 00360305000104. Contratado : CAIXA ECONOMICA FEDERAL -.Objeto: Prorrogar o prazo de vigência do Contrato original e incluir a SUBCLÁUSULA SEGUNDA na CLÁUSULA PRIMEIRA. Fundamento Legal: Lei nº 8666/93. Vigência: 15/01/2018 a 15/01/2019. Data de Assinatura: 15/01/2018.

(SICON - 18/01/2018)

AVISO DE REVOGAÇÃO PREGÃO ELETRÔNICO Nº 7/2017

Fica revogada a licitação supracitada, referente ao processo Nº 55000000573201609. Objeto: Pregão Eletrônico - Aquisição de licença de uso de firewall existente na Secretaria de Especial de Agricultura Familiar e do Desenvolvimento Agrário do respectivo fabricante e modelo Check Point, Account ID 0006936899, incluindo implantação, garantia, treinamento, módulo de Gerência centralizada da solução, transferência de conhecimento e suporte técnico on-site, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

JONATHAS BARBOSA DO AMARAL
Pregoeiro

(SIDEC - 18/01/2018) 110703-00001-2017NE800085

SUBSECRETARIA DE REORDENAMENTO AGRÁRIO

RETIFICAÇÃO

No extrato de publicação do Convênio nº 862523/2017, publicado no D.O.U. de 09/01/2018, pg. 109, Seção 3, onde se lê: "Convenente: JOSE GUILHERME TOLLSTADIUS LEAL CPF nº 702.317.376-53", leia-se: "Convenente: ARGILEU MARTINS DA SILVA CPF nº 473.494.256-00".

SECRETARIA-GERAL
SECRETARIA DE ADMINISTRAÇÃO

EXTRATO DE CONTRATO Nº 11/2018 - UASG 110001

Nº Processo: 00087000505201718. DISPENSA Nº 61/2017. Contratante: PRESIDENCIA DA REPUBLICA -.CNPJ Contratado: 38008405000149. Contratado : EMPLAC COMERCIO DE PLACAS PARA -VEICULOS LTDA - EPP. Objeto: Fornecimento, sob demanda, de placas comuns para veículos. Fundamento Legal: LEI 8.666/93 . Vigência: 16/01/2018 a 31/12/2018. Valor Total: R$1.800,00. Fonte: 100000000 - 2018NE800025. Data de Assinatura: 16/01/2018.

(SICON - 18/01/2018) 110001-00001-2018NE800077

EXTRATO DE CONTRATO Nº 55/2017 - UASG 110001

Nº Processo: 00094001674201786. PREGÃO SRP Nº 26/2017. Contratante: PRESIDENCIA DA REPUBLICA -.CNPJ Contratado: 72381189000625. Contratado : DELL COMPUTADORES DO BRASIL LTDA -.Objeto: Fornecimento de microcomputadores. Fundamento Legal: Lei nº 8.666/93 . Vigência: 29/12/2017 a 26/06/2018. Valor Total: R$1.650.000,00. Fonte: 100000000 - 2017NE803348. Data de Assinatura: 29/12/2017.

(SICON - 18/01/2018) 110001-00001-2018NE800077

RESULTADO DE JULGAMENTO PREGÃO Nº 57/2017

Sagrou-se vencedora do certame a empresa: CHIP7 DE INFORMÁTICA ELETRO ELETRÔNICOS LTDA - ME, CNPJ nº 20.115.087/0001-50, item único, no valor total de R$ 27.192,00

DIEGO FERNANDES DO NASCIMENTO
Pregoeiro/PR

(SIDEC - 18/01/2018) 110001-00001-2018NE800077

EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A.

EXTRATO DE CONTRATO Nº 19/2017 - UASG 395001

Nº Processo: 70840000238201778. PREGÃO SRP Nº 100/2016. Contratante: EMPRESA DE PLANEJAMENTO E -LOGISTICA S.A - EPL. CNPJ Contratado: 05407609000101. Contratado : ALTAS NETWORKS & TELECOM LTDA - Objeto: Contratação de solução de alta disponibilidade de next generation firewall com gerenciamento centralizado e integrado, atualizações de proteção e suporte técnico, 24x7, pelo prazo de 36 meses, incluindo serviços de instalação e treinamento, que serão prestados nas condições estabelecidas no Termo de Referência do Edital 100/2016 da UFSJ, UASG 154069. Fundamento Legal: Lei 10520/2002, Dec 7892/2013, Dec 2271/97, IN SLTI/MP 04/2014, IN/SLTI 02/2008 e Lei 8666/93 . Vigência: 26/12/2017 a 25/12/2020. Valor Total: R$294.000,00. Fonte: 100000000 - 2017NE800261. Data de Assinatura: 26/12/2017.

(SICON - 18/01/2018) 395001-39253-2018NE800006

EMPRESA BRASIL DE COMUNICAÇÃO S/A

EXTRATO DE TERMO ADITIVO

Espécie: Termo Aditivo nº 02 ao Contrato de Prestação de Serviços Continuados de Produção e Transmissão de Sinal de Televisão por Satélite EBC/COORD-CM/Nº 0078/2015. Contratante: Empresa Brasil de Comunicação S/A - EBC. Contratada: Valle Telecomunicações Ltda-EPP, CNPJ/MF: 04.768.527/0001-11. Objeto: Prorrogar o prazo de vigência do Contrato Original e discriminar os dados da Nota de Empenho do Exercício Financeiro de 2017. Do valor anual para a prorrogação: R$ 4.148.000,00. Dos Recursos Orçamentários para prorrogação: Programa de Trabalho: 24722210126750001 (Comunicação e Transmissão de Atos e Fatos do Governo Federal). Elemento de Despesa: 339039 (Outros Serviços de Terceiros - Pessoa Jurídica). Nota de Empenho: 2017NE002836. Emissão: 10/11/2017. Valor: R$ 138.266,66. Vigência: 18/12/2017 a 18/12/2018. Assinatura: 18/12/2017. Processo: 1174/2015.

SECRETARIA DE GOVERNO
SECRETARIA NACIONAL DE JUVENTUDE

EXTRATOS DE CONVÊNIOS

Espécie: Convênio Nº 861463/2017, Nº Processo: 00019001130201717, Concedente: Presidência da República, Convenente: MUNICIPIO DE IMPERATRIZ CNPJ nº 06158455000116, Objeto: Implantar e implementar o Programa Estação Juventude, na modalidade complementar Estação Juventude como espaço acolhedor para juventude, no município de Imperatriz - MA, localizado no Complexo esportivo Recanto Universitário, na Rua do Cravo S/N, Vila Fiquene, equipado e com pessoal capacitado, para atender jovens na faixa de 15 a 29 anos, oferecendo serviços e ações que ampliem o

Empresa de Planejamento e Logística
Fls. 210
Rubrica
EPL

ATA DA 16ª REUNIÃO EXTRAORDINÁRIA REALIZADA EM 26 DE DEZEMBRO DE 2017

Aos vinte e seis dias do mês de dezembro de 2017, às 11h, na sede da Empresa de Planejamento e Logística S/A, no SCS, Quadra 9, Lote "C", 8º andar, Edifício Parque Cidade Corporate, CEP 70.308-200, Brasília-DF, compareceram os membros da Diretoria Executiva (DIREX), eleitos conforme o Estatuto Social. Presentes o Diretor-Presidente, **Sr. José Carlos Medaglia Filho**; o Diretor de Gestão, **Sr. Maurício Pereira Malta**; a Gerente Substituta da Procuradoria Jurídica, Sra. Andrea Vieira Andreis; e a Secretária *Ad hoc* da DIREX, Sra. Marina F. H. Amantéa. Presente o quórum exigido pelo artigo 26 do Estatuto Social da EPL, foi declarada aberta a sessão, ocasião em que os membros da DIREX entenderam por abrir mão do prazo estipulado no art. 31 do mesmo diploma, tendo em vista que, embora a íntegra do material que instrui a proposta não tenha sido disponibilizado com a antecedência prevista, trata-se de tema relevante, cuja evolução foi acompanhada pelos Diretores, razão pela qual se entende pela viabilidade de compreensão e deliberação sobre os temas objeto da presente Pauta. **ITEM 1. DELIBERAÇÕES: SUBITEM 1.1. Nota Técnica nº 36/2017-GELIC/DGE, de 29.12.2017, da Gerência de Licitações e Contratos, aprovada pelo Diretor de Gestão (Processo nº 50840.000238/2017-78):** Proposta de alteração da minuta de contrato aprovada na 19ª Reunião Ordinária da DIREX, realizada em 7 de dezembro de 2017, para exclusão da cláusula sétima que trata da garantia de 5% sobre o valor total do contrato, considerando que este custo não estava contemplado no Pregão Eletrônico nº 100/2016, da Fundação Universidade Federal de São João Del-Rei, e, portanto, não foi aceito pela empresa a ser contratada. **Deliberação do SUBITEM 1.1.** Tratando-se de tema da alçada da DIREX, considerando as informações apresentadas na Nota Técnica nº 36/2017-GELIC/DGE, os membros autorizaram, por unanimidade, a exclusão da cláusula sétima da minuta contratual aprovada na 19ª reunião da DIREX. Registra-se que a Gerente Substituta da Procuradoria Jurídica manifestou que não há óbice jurídico para exclusão da cláusula, sendo, portanto, um ato de gestão. Concluída a deliberação, evoluiu-se ao **ITEM 2. ENCERRAMENTO:** Sem mais registros, o Diretor-Presidente encerrou os trabalhos e determinou a lavratura da presente Ata, que segue assinada pelos presentes.

JOSÉ CARLOS MEDAGLIA FILHO
Diretor-Presidente

MAURÍCIO PEREIRA MALTA
Diretor de Gestão

MARINA F. H. AMANTÉA.
Secretária *Ad hoc*

EM BRANCO

CONTRATO ADMINISTRATIVO N.º 19/2017 CELEBRADO ENTRE A EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A – EPL E A EMPRESA ALTAS NETWORKS & TELECOM LTDA PARA CONTRATAÇÃO DE SOLUÇÃO DE ALTA DISPONIBILIDADE DE *NEXT GENERATION FIREWALL – NGFW* COM GERENCIAMENTO CENTRALIZADO E INTEGRADO, ATUALIZAÇÕES DE PROTEÇÃO E SUPORTE TÉCNICO, 24X7, PELO PRAZO DE 36 MESES, INCLUINDO SERVIÇOS DE INSTALAÇÃO E TREINAMENTO.

CONTRATANTE: EMPRESA DE PLANEJAMENTO E LOGÍSTICA S.A. - EPL, inscrita no CNPJ (MF) n.º 15.763.423/0001-30, e Inscrição Estadual GDF nº 07.622.898/001-15, com sede no Setor Comercial Sul, Quadra 9, Lote C, Complexo Parque Cidade Corporate, Torre C – 7º e 8º andares, em Brasília/DF, CEP 70308-200, representada pelo Diretor de Gestão, Senhor **MAURÍCIO PEREIRA MALTA**, brasileiro, casado, portador da RG nº 1243998-SSP/ES e do CPF n.º 507.460.655-15, nomeado pela Ata da 8ª Reunião Extraordinária do Conselho de Administração de 22 de dezembro de 2016, e pelo Diretor Presidente, Senhor **JOSE CARLOS MEDAGLIA FILHO**, brasileiro, casado, engenheiro civil, portador da Carteira de identidade RG nº 2.916.693 SSP/DF e inscrito no CPF/MF sob o nº 388.908.520-20, domiciliado em Brasília – DF, nomeado pela Ata da 7ª Reunião Extraordinária do Conselho de Administração de 2 de agosto de 2016.

CONTRATADA: ALTAS NETWORKS & TELECOM LTDA, inscrita no CNPJ sob o nº 05.407.609/0001-01, Inscrição Estadual MG nº 062.212.833-0032, com sede na Rua Juruá nº 46, 7º andar, salas 704 a 708 – Bairro da Graça, Belo Horizonte, MG, CEP: 31.140-020, neste ato representado pelo Senhor **ALMIR FRANZ DE LIMA,** brasileiro, casado, portador da Cédula de Identidade nº MG -2.880.975, SSP/MG, inscrito no CPF(MF) sob o nº 591.914.736-91, de acordo com a representação legal que lhe é outorgada por Contrato Social.

Os CONTRATANTES têm entre si justo e avençado, e celebram o presente contrato, tendo

em vista o que consta no Processo nº 50840.000238/2017-78 e em observância às disposições da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 7.892, de 23 de janeiro de 2013, do Decreto nº 2.271, de 7 de julho de 1997, da Instrução Normativa SLTI/MP nº 04/2014 e suas alterações, da Instrução Normativa SLTI/MPOG n° 02, de 2008 e subsidiariamente na Lei 8.666, de 21 de junho de 1993, e demais normas correlatas, decorrente da adesão à Ata de Registro de Preços oriunda do Pregão nº 100/2016 da Fundação Universidade Federal de São João Del-Rei - UFSJ, UASG: 154069, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. CONTRATAÇÃO DE SOLUÇÃO DE ALTA DISPONIBILIDADE DE *NEXT GENERATION FIREWALL – NGFW* COM GERENCIAMENTO CENTRALIZADO E INTEGRADO, ATUALIZAÇÕES DE PROTEÇÃO E SUPORTE TÉCNICO, 24X7, PELO PRAZO DE 3(MESES, INCLUINDO SERVIÇOS DE INSTALAÇÃO E TREINAMENTO, que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital do Pregão Eletrônico nº 100/2016 da Fundação Universidade Federal de São João Del-Rei, UASG: 154069.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão Eletrônico nº 100/2016 da Fundação Universidade Federal de São João Del-Rei, UASG: 154069, identificado no preâmbulo e à proposta da contratada, independentemente de transcrição.

1.3. Este Contrato vincula-se ao Termo de Referência constante das fls. 131/150 do Processo 50840.000238/2017-78.

1.4. Objeto da contratação:

Itens do Processo	Descrição	Unidade	Quantitativo a ser contratado
4	Firewall	unidade	2
9	Software de relatórios	licença	1

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Contrato é de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, tendo eficácia após publicado o respectivo extrato na Imprensa Oficial, improrrogáveis.

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor da contratação é de **R$ 294.000,00 (duzentos e noventa e quatro mil reais),** conforme tabela abaixo:

ITEM	DESCRIÇÃO	QUANT.	UND.	VALOR UNITÁRIO	VALOR TOTAL
4	FIREWALL	2	UNIDADE	125.000,00	250.000,00
9	SOFTWARE	1	Licença	44.000,00	44.000,00
Total					**R$ 294.000,00**

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2017, na classificação abaixo:

Gestão/Unidade: 395001
Fonte: 100
Elemento de Despesa: 4490
PI: 26.121.2101.20UA.0001

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O pagamento será realizado no prazo máximo de 15 (quinze) dias úteis, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agencia e conta indicado pela Contratada.

5.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

5.3. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 03 (três) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

5.4. O pagamento somente será autorizado depois de efetuado o "atesto" pela fiscalização do contrato, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados.

5.5. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

5.6. Nos termos do artigo 36, § 6°, da Instrução Normativa SLTI/MPOG n° 02, de 2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

5.6.1. não produziu os resultados acordados;

5.6.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

5.6.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

5.7. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

5.8. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

5.9. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

5.10. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

5.11. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

5.12. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao

ALTAS NETWORKS

5.13. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante, não será rescindido o contrato em execução com a contratada inadimplente no SICAF.

5.14. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

5.14.1. A Contratada regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

5.15. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$$EM = I \times N \times VP$$

Onde:

EM = Encargos Moratórios.

VP = Valor da parcela a ser paga.

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.

I = índice de compensação financeira = 0,0001644, assim apurado:

$$\frac{I = (TX)}{365} \qquad \frac{I = (6/100)}{365} \qquad I = 0{,}0001644$$

TX = Percentual da taxa anual = 6%

6. CLÁUSULA SEXTA – INEXISTÊNCIA DE REAJUSTE

6.1. O preço é fixo e irreajustável.

7. CLÁUSULA SÉTIMA - DA GARANTIA TÉCNICA

7.1. O objeto deste contrato deverá contar com a Garantia Técnica, nos termos do item 5.10 do Termo de Referência constante das fls. 131/150 do Processo 50840.000238/2017-78.

8. CLÁUSULA OITAVA – REGIME DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. O regime de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de

Referência, anexo do Edital do Pregão Eletrônico nº 100/2016 da Fundação Universidade Federal de São João Del-Rei, UASG: 154069.

8.2. O objeto desta contratação deverá ser executado em exata observância no Termo de Referência constante das fls. 131/150 do Processo 50840.000238/2017-78.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. São obrigações da CONTRATANTE:

a) receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

b) verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

c) comunicar à contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

d) acompanhar e fiscalizar o cumprimento das obrigações da contratada, através de comissão/servidor especialmente designado; e

e) efetuar o pagamento à contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital da licitação e seus anexos;

9.2. A Administração não responderá por quaisquer compromissos assumidos pela contratada com terceiros, ainda que vinculados à execução do Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos ou subordinados.

9.3. São Obrigações da CONTRATADA

9.4. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

a) efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

b) O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada;

ALTAS NETWORKS

c) responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

d) substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

e) comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

f) manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação; e

g) indicar preposto para representá-la durante a execução do contrato;

9.5. A contratada deverá prestar serviços de manutenção e suporte técnico a todos os produtos contratados, no local de instalação da solução, sem ônus para a EPL, durante os sete dias da semana, incluindo finais de semana e feriados, 24 (vinte e quatro) horas por dia (7x24), conforme condições e prazos previstos do Edital da licitação e neste documento.

10. CLÁUSULA DÉCIMA – SANÇÕES ADMINISTRATIVAS.

10.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

a) inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
b) ensejar o retardamento da execução do objeto;
c) fraudar na execução do contrato;
d) comportar-se de modo inidôneo;
e) cometer fraude fiscal;
f) não mantiver a proposta.

10.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

b) multa moratória de 0,1% (um décimo por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 2% (dois por centos);

c) multa compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

d) em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

e) suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 anos.

f) declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base na alínea anterior.

10.3. A sanção estabelecida na alínea "f", subitem 11.2 é de competência exclusiva do Ministro de Estado, facultada a defesa da CONTRATADA no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

10.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

a) tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

10.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

10.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

10.7. As penalidades serão obrigatoriamente registradas no SICAF.

ALTAS NETWORKS

11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas neste Contrato.

11.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

11.4. O termo de rescisão, sempre que possível, será precedido:

11.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES

12.1. É vedado à CONTRATADA:

12.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

12.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessária, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.2.1. É vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666, de 1993.

13.3. As supressões resultantes de acordo celebrados entre as contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.4. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da EPL quanto à continuidade do contrato.

14. CLÁUSULA DÉCIMA QUARTA – DA SUBCONTRATAÇÃO

14.1. Não será admitida a subcontratação do objeto contratado

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1 Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

17.1. O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Seção Judiciária de. Brasília-DF - Justiça Federal.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

Brasília, 26 de dezembro de 2017.

JOSE CARLOS MEDAGLIA FILHO
DIRETOR PRESIDENTE

MAURÍCIO PEREIRA MALTA
DIRETOR DE GESTÃO

ALMIR FRANZ DE LIMA
CONTRATADA

TESTEMUNHAS:

NOME:
CPF:
RG n.º:

Andrea Abrão Paes Leme
Mat. SIAPE nº 1990146
EPL

NOME:
CPF:
RG n.º:

Eduardo Solano Spim
Mat. SIAPE Nº: 2028629
EPL

1. DEFINIÇÃO E ESPECIFICAÇÕES TÉCNICAS MÍNIMAS NECESSÁRIAS

1.1. Appliance de firewall

1.1.1. Características de hardware e performance:

- *Throughput* de, no mínimo, 24 Gbps com a funcionalidade de *firewall* habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
- Suporte a, no mínimo, 5 milhões de conexões simultâneas;
- Suporte a, no mínimo, 270 mil novas conexões por segundo;
- Throughput de, no mínimo, 16 Gbps de VPN IPSec;
- Estar licenciado para ou suportar sem o uso de licença, 2 mil túneis de VPN IPSEC Site-to-Site simultâneos;
- Estar licenciado para ou suportar sem o uso de licença, 10 mil túneis de clientes VPN IPSEC simultâneos;
- Throughput de, no mínimo, 2.2 Gbps de VPN SSL;
- Suporte a, no mínimo, 5 mil clientes de VPN SSL simultâneos;
- Suportar no mínimo 4 Gbps de throughput de IPS;
- Suportar no mínimo 3.5 Gbps de throughput de Inspeção SSL;
- Throughput de, no mínimo, 2.4 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- Possuir ao menos 16 interfaces 1Gbps;
- Possuir ao menos 2 interfaces 10Gbps;
- Disco de, no mínimo, 120 GBytes para armazenamento de informações locais
- Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
- Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

1.1.2. Requisitos mínimos de funcionalidade:

- A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall-NGFW, e console de gerência e monitoração;
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- O software deverá ser fornecido em sua versão mais atualizada;
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede;
- Os dispositivos de proteção de rede devem possuir suporte a 1024 VLAN Tags 802.1q;
- Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP;
- Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- Deve suportar NAT dinâmico (Many-to-1);
- Deve suportar NAT dinâmico (Many-to-Many);
- Deve suportar NAT estático (1-to-1);
- Deve suportar NAT estático (Many-to-Many);
- Deve suportar NAT estático bidirecional 1-to-1;
- Deve suportar Tradução de porta (PAT);
- Deve suportar NAT de Origem;

ALTAS NETWORKS LICITAÇÃO

- Deve suportar NAT de Destino;
- Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- Deve suportar NAT64 e NAT46;
- Deve implementar o protocolo ECMP;
- Deve implementar balanceamento de link por hash do IP de origem;
- Deve implementar balanceamento de link por hash do IP de origem e destino;
- Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
- Deve suportar o balanceamento de, no mínimo, quatro links;
- Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- Enviar log para sistemas de monitoração externos, simultaneamente;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- Proteção anti-spoofing;
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- Suportar OSPF graceful restart;
- Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
- A configuração em alta disponibilidade deve sincronizar: Sessões;
- A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
- A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
- A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
- O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- A utilização dos dispositivos em alta disponibilidade não deve impor limitações quanto à utilização de sistemas virtuais (contextos);
- Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
- O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
- Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolação das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
- As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, o licenciamento do dispositivo de segurança não pode ter nenhuma relação com sua configuração de rede como, mas não limitado a, configuração de interfaces, endereços

lógicos, etc , podendo ser utilizado por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *software* com o fabricante.

- Deverá suportar controles por zona de segurança;
- Controles de políticas por porta e protocolo;
- Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
- Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
- Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- Controle de inspeção e de-criptografia de SSH por política;
- Suporte a objetos e regras IPV6;
- Suporte a objetos e regras multicast;
- Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

1.1.3. **Controle de aplicações:**

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software,

protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

- Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over, http, gotomeeting, webex, evernote, google-docs, etc;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
- Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;
- Identificar o uso de táticas evasivas via comunicações criptografadas;
- Atualizar a base de assinaturas de aplicações automaticamente;
- Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

ALTA NETWORKS LICITAÇÃO

- Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MSSQL, IMAP, DNS, LDAP, RTSP e SSL;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook, Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon3, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Categoria da aplicação

- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: Aplicações que usem técnicas evasivas, utilizadas por malwares como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos, etc.

1.1.4. **Prevenção de ameaças:**

- Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
- As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura;
- Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve incluir proteção contra ataques de negação de serviços;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de padrões de estado de conexões;

ALTAS NETWORKS LICITAÇÃO

- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise heurística;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- Detectar e bloquear a origem de portscans;
- Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- Possuir assinaturas para bloqueio de ataques de buffer overflow;
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e antispyware, permitindo a criação de exceções com granularidade nas configurações;
- Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Identificar e bloquear comunicação com botnets;
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação;
- Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

- Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- Proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

1.1.5. **Filtro de URL:**

- Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- Possuir pelo menos 60 categorias de URLs;
- Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- Permitir a customização de página de bloqueio;
- Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).

1.1.6. **Identificação de usuários:**

- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
- Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
- Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

1.1.7. **QoS e Traffic Shaping:**

- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
- Suportar a criação de políticas de QoS e Traffic Shaping por porta;
- O QoS deve possibilitar a definição de classes por Banda Garantida;
- O QoS deve possibilitar a definição de classes por Banda Máxima;
- O QoS deve possibilitar a definição de classes por Fila de Prioridade
- Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

1.1.8. **Filtro de dados:**

- Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1.1.9. **Geo Localização:**

- Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

1.1.10. **VPN:**

- Suportar VPN Site-to-Site e Cliente-To-Site;
- Suportar IPSec VPN;
- Suportar SSL VPN;
- A VPN IPSEc deve suportar 3DES;
- A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN;
- IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

- A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- Atribuição de DNS nos clientes remotos de VPN;
- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- Suportar leitura e verificação de CRL (certificate revocation list);
- Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SCCM, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário;
- Deverá manter uma conexão segura com o portal durante a sessão;
- O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows XP (32 bit), Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

1.1.11. **Condições operacionais:**

- Alimentação / tensão de 100-240 VAC;
- Possuir conector para fonte de alimentação externa redundante;
- Alimentação / frequência de 50/60 Hz;
- Temperatura - faixa de operação de 0° a 40° C.

1.2. Software de relatórios

1.2.1. Características gerais

- Deve ser do mesmo fabricante dos itens de firewall, a fim de garantir compatibilidade;
- Deve estar licenciado para coletar logs e gerar relatório de múltiplos firewalls;
- Possuir capacidade receber ao menos 5GBytes de logs diários;
- Caso a solução de coleta de logs e relatórios seja ofertada em appliance físico deverá possuir ao menos 4 interfaces de 1Gbps RJ-45, 16GB de memória RAM, um processador octacore e ao menos 3 TB de armazenamento configurados em RAID 1;
- Caso a solução de gerenciamento seja ofertada em appliance virtual deverá ser compatível com ambiente VMware ESXi 5.5, estar licenciado para pelo menos 3 TB de espaço em disco e não deve possuir limite para suporte a expansão de memória RAM caso virtual;

1.2.2. Funcionalidades gerais:

- Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução;
- Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH);
- Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração;
- Suportar SNMP versão 2 e versão 3 na solução de relatórios;
- Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;
- Deve permitir a criação de administradores que acessem à todas as instâncias de virtualização da solução de relatórios;
- Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;
- Autenticação integrada a servidor Radius;
- Geração de relatórios com mapas geográficos ou modo tabela gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- Autenticação integrada ao Microsoft Active Directory;

- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha do mesmo;
- Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado;
- Possuir mecanismo para que logs antigos sejam removidos automaticamente;
- Permitir a importação e exportação de relatórios;
- Deve ser possível exportar os logs em CSV;
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar;
- A solução deve possuir relatórios pré-definidos;
- Possuir envio automático de logs para um servidor FTP externo a solução;
- Possibilitar a duplicação de relatórios existentes e edita-los Possuir a capacidade de personalização de capas para os relatórios;
- Possibilitar a duplicação de gráficos existentes de relatórios;
- Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log;
- Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados;
- Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios;
- Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime;
- Dever ser possível fazer download dos arquivos de logs recebidos;
- Deve possuir agendamento para gerar e enviar automaticamente relatórios;
- Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades;
- Permitir o envio de maneira automática de relatórios por email;
- Deve permitir a escolha do email a ser enviado para cada relatório escolhido;
- Permitir programar a geração de relatórios, conforme calendário definido pelo administrador;

- Deve ser possível definir filtros nos relatórios;
- Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;
- Permitir que relatórios criado sejam no idioma Português;
- Gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros;
- Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
- Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;
- Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros;
- Deve possuir a informação de Indicador de Compromisso (IoC);
- Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o objetivo de detectar problemas de performance de sistema de acordo com o relatório criado;
- Permitir que a solução busque log arquivados de outros dispositivos da mesma solução;
- Deve possuir relatório de PCI DSS Compliance;
- Deve ser possível definir o espaço que cada instância de virtualização poderá utilizar para armazenamento de logs;
- A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes;
- Deve suportar duplo fator de autenticação (token) para os administradores do sistema de relatórios;
- Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo e caracteres a usar;
- Deve permitir ver em tempo real os logs recebidos.

Empresa de Planejamento e Logística

Empresa de Planejamento e Logística Fls. 224 Rubrica EPL

ANEXO B

TERMO DE COMPROMISSO DA MANUTENÇÃO DE SIGILO

A Empresa **ALTAS NETWORKS & TELECOM LTDA**, inscrita no CNPJ sob o n.º 05.407.609/0001-01, sediada na Rua Juruá nº 46, 7º andar, salas 704 a 708 – Bairro da Graça, Belo Horizonte, MG, CEP: 31.140-020, por intermédio de seu representante legal, Senhor **ALMIR FRANZ DE LIMA,** brasileiro, casado, portador da Cédula de Identidade n.º MG -2.880.975, expedida pela(o) SSP/MG e CPF n.º 591.914.736-91, **DECLARA** para fins de celebração da contratação com a Empresa de Planejamento e Logística – EPL, CNPJ nº 15.763.423/0001-30, que se compromete a **manter em sigilo**, ou seja, não revelar ou divulgar as informações da EPL, ou de seus empregados, obtidas em razão da execução contratual, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de seu conhecimento. A empresa está ciente que, caso tenha acesso à base de informações da EPL inserida no sistema, ela deverá preservar tais informação e, em nenhuma hipótese, divulgá-las sem autorização formal da EPL. A Empresa declara, ainda, que dará ciência aos seus empregados sobre a obrigação de manter sigilo sobre as informações obtidas em razão da execução contratual em pauta.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar a EPL de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, danos, perdas, custas e despesas que porventura venha sofrer como resultado da violação do disposto neste instrumento.

ALMIR FRANZ DE LIMA
CONTRATADA
RG: MG -2.880.975 – SSP/MG
CPF: 591.914.736-91

Empresa de Planejamento e Logística

ANEXO E

TERMO DE RECEBIMENTO DEFINITIVO

Processo nº:	**Contrato nº:**
Objeto:	**Vigência:**
Contratada:	**CNPJ:**
Licenças:	
Valor:	
Data prevista para entrega:	
Data da efetiva entrega:	

Por este instrumento, atesto, para fins de cumprimento do disposto no art. 34, inciso VIII, da Instrução Normativa SLTI/MP nº 4/2014, a Aquisição de uma solução de descoberta de dados (Data Discovery), com licenças de software de uso perpétuo, em conjunto com os serviços de instalação e configuração, suporte técnico e atualização de versão, treinamento (capacitação técnica) e de suporte especializado, conforme Lista de Verificação anexa.

Os fornecimentos das licenças foram adquiridos de forma satisfatória, razão pela qual lavramos este TERMO DE RECEBIMENTO DEFINITIVO, para os fins legais e para efeitos de pagamento.

De acordo,

Brasília, de de 2017.

Fiscal Requisitante	**Gestor**
Preposto da Contratada	
Assinatura **RG Nº**	

Empresa de Planejamento e Logística

Empresa de Planejamento e Logística
Fls. 226
Rubrica
EPL

ANEXO F
LISTA DE VERIFICAÇÃO

Contrato:	**Mês de Referência:**	**Período Verificado:**
RECEBIMENTO DEFINITIVO		
Item	**Aceite**	
Disponibilização de acesso da EPL ao Sistema		
Realização da Instalação		
Disponibilização do suporte técnico do Sistema à EPL.		
Conformidade do Atendimento do Suporte Técnico		
Funcionamento e disponibilidade plena e diária do Sistema no mês de faturamento		
Atendimento das necessidades da contabilidade pela solução		
Cumprimento de Prazos		
Cumprimento das obrigações contratuais		
Verificação da Regularidade Fiscal, Trabalhista e Previdenciária da contratada		
Data da Verificação:	**Data da Verificação:**	
Assinatura **Fiscal Requisitante** **Assinatura** **Gestor**		

3) No campo "Aceite", marcar "atende", "não atende", ou "conforme relatório anexo" (detalhar ajustes de pagamento, desconformidades, dentre outros em relatório anexado à lista).

4) A lista de verificação é instrumento da Equipe de Fiscalização e poderá ser alterada conforme suas necessidades ao longo da vigência da contratação.

Empresa de Planejamento e Logística

ANEXO G

MODELO DE ORDEM DE SERVIÇO

A Empresa de Planejamento e Logística – EPL, por meio do servidor (*nome*), matrícula SIAPE (*número*), e em face do Contrato em epígrafe, requer à Empresa (*nome*), CNPJ (*número*), endereço (*indicar*), telefone (*indicar*), e-mail (*indicar*), a disponibilização do Software, conforme abaixo indicado:

Software a ser fornecido: (*indicar*)

Quantidades de licenças : (*indicar*)

Prazo: (*indicar*)

Endereço: (*indicar*)

_____

Nome/carimbo e Assinatura do Servidor

Recebi, em ___/___/____, a presente Ordem de Serviço, obrigando-me desde já a realizar o serviço dela constante, no prazo e valor acima indicado.

_____

Nome e Assinatura do Responsável Legal pela Contratada

RG e CPF