JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DE GOIÁS

ATA DE REGISTRO DE PREÇOS
Nº 42/2019

O TRIBUNAL REGIONAL ELEITORAL DE GOIÁS (TRE-GO), órgão do Poder Judiciário da União, inscrito no CNPJ sob o nº 05.526.875/0001-45, com sede na Praça Cívica nº 300 Centro, nesta Capital, neste ato representado por seu Diretor Geral, Sr. WILSON GAMBOGE JÚNIOR, RG nº 2.986.181, expedida pela SSP/GO, inscrito no Cadastro de Pessoas Físicas do Ministério da Fazenda – CPF/MF sob o nº 799.305.061-87, considerando a homologação da licitação na modalidade de pregão, forma eletrônica, nº 54/2019, publicada no DOU de 18/11/2019, processo administrativo nº 2315/2019, RESOLVE registrar os preços da empresa indicada e qualificada nesta ATA, de acordo com a classificação por ela alcançada e na quantidade cotada, atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes das Leis nº 8.666, de 21 de junho de 1993, e nº 10.520, de 17 de julho de 2002, e dos Decretos nº 5.450, de 31 de maio de 2005, e nº 7.892, de 23 de janeiro de 2013, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente ata tem por objeto o registro de preços para eventual aquisição de solução de Tecnologia da Informação, para Segurança e Conectividade da Rede de Dados, visando a atualização e a manutenção da infraestrutura de comunicação de dados entre os usuários e os serviços de TI utilizados no TRE-GO, com garantia e suporte técnico, conforme as especificações, condições e prazos constantes do Edital do Pregão Eletrônico TRE-GO nº 54/2019 e seus anexos, que são parte integrante deste instrumento, independentemente de transcrição.

2. DA EMPRESA BENEFICIÁRIA

2.1. É beneficiária desta Ata de Registro de Preços, a sociedade empresária **ARVVO TECNOLOGIA, CONSULTORIA E SERVIÇOS LTDA**, CNPJ nº 25.359.140/0001-81, com sede em SHN Qd 01 Conj A Bl A salas 1114 e 1115, Edifício Le Quartier, Brasília-DF CEP: 70701-010, telefone nº (61) 3553-9006, e-mail contato@arvvo.com.br, representada por seu sócio administrador, Senhor André Luiz Alves de Oliveira, RG 1.685.233, expedido por SSP-DF, inscrito no Cadastro de Pessoas Físicas do Ministério da Fazenda – CPF/MF sob o nº 705.590.401-30.

3. DOS QUANTITATIVOS E DOS PREÇOS REGISTRADOS

3.1. Os quantitativos e os preços registrados no presente instrumento são os seguintes:

	ITEM	DESCRIÇÃO	QUANTIDADE REGISTRADA	VALOR UNITÁRIO (R$)
LOTE 2	7	Roteador Firewall/Gateway.	2	615.000,00
	8	Upgrade de licença de software de gerencia.	1	133.500,00
	9	Serviços de instalação e configuração dos equipamentos.	1	40.000,00

3.2. A Administração realizará pesquisa de mercado periodicamente, em intervalos não superiores a 180 (cento e oitenta) dias, a fim de verificar a vantajosidade dos preços registrados nesta Ata.

4. ÓRGÃO GERENCIADOR E ÓRGÃO(S) PARTICIPANTE(S)

4.1. O órgão gerenciador desta ata será o TRIBUNAL REGIONAL ELEITORAL DE GOIÁS;

4.2. Não existem órgãos participantes do presente registro de preços.

5. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

5.1. Poderão utilizar-se da Ata de Registro de Preços, na qualidade de órgão não participante do certame, apenas os Tribunais Regionais Eleitorais, o Tribunal Superior Eleitoral e os órgãos e entidades que integram o FORJUS (Fórum Permanente do Sistema de Justiça em Goiás), mediante anuência do órgão gerenciador, desde que devidamente justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas na Lei nº 8.666/1993 e no Decreto nº 7.892/2013.

5.1.1. A restrição acima imposta visa assegurar o princípio da vinculação ao edital, a cooperação entre os Órgãos da Justiça Eleitoral e daqueles que integram o Sistema de Justiça no Estado de Goiás.

5.1.2. Os órgãos acima indicados, quando desejarem utilizar esta ata, deverão consultar o TRE-GO para manifestação sobre a possibilidade de adesão, nos termos do artigo 22, § 1º, do Decreto nº 7.892/2013.

5.1.3. A manifestação do órgão gerenciador, de que trata o subitem anterior, fica condicionada à realização de estudo, pelos órgãos e pelas entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública federal da utilização da ata de registro de preços, conforme estabelecido em ato do Secretário de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão.

5.2. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.

5.3. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

5.4. As adesões à ata de registro de preços são limitadas, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que eventualmente aderirem.

5.5. Ao órgão não participante que aderir à ata competem os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação as suas próprias contratações, informando as ocorrências ao órgão gerenciador.

5.6. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços.

5.7. Caberá ao órgão gerenciador autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência da ata, desde que solicitada pelo órgão não participante.

6. DA ASSINATURA DO TERMO DE CONTRATO E DA SOLICITAÇÃO DOS SERVIÇOS

6.1. Para execução desta ata de registro de preços, o TRE-GO convocará a empresa cujo preço foi registrado em primeiro lugar para assinatura do termo de contrato correspondente.

6.2. A empresa beneficiária quando convocada ficará obrigada a atender todos os pedidos efetuados pelo órgão gerenciador e pelos partícipes, se houver, durante a validade desta ata de registro de preços.

6.3. Ao assinar a ata de registro de preços, a empresa beneficiária obriga-se a prestar os serviços conforme especificações e demais condições contidas no Edital do Pregão Eletrônico TRE-GO nº 54/2019 e seus anexos e na proposta de preços apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital.

6.4. Quando a empresa beneficiária da Ata se recusar a assinar o termo de contrato, sem justificativa, seu registro será cancelado nos termos do artigo 20, inciso II, do Decreto nº 7.892/2013, sem prejuízo das penalidades cabíveis.

6.4.1. Nesse caso, serão convocadas as demais empresas registradas no cadastro de reserva, na ordem de classificação, conforme o disposto no art. 11, § 1º, do **Decreto 7.892/2013.**

7. DAS OBRIGAÇÕES DAS PARTES

7.1. Constituem obrigações do TRE-GO, além das especificadas no Edital do Pregão Eletrônico TRE-GO nº 54/2019 e seus anexos:

7.1.1. Gerenciar a ata de registro de preços, providenciando a indicação, sempre que solicitado, da empresa registrada, para atendimento às necessidades da Administração, obedecendo os quantitativos definidos no Edital do Pregão Eletrônico TRE-GO nº 54/2019;

7.1.2. Notificar a empresa registrada para assinar o termo de contrato;

7.1.3. Promover ampla pesquisa de mercado, de forma a verificar se os preços registrados permanecem compatíveis com os praticados;

7.1.4. Conduzir os procedimentos relativos a eventuais negociações dos preços registrados e à aplicação de penalidades por descumprimento do pactuado nesta ata de registro de preços, em relação às suas próprias contratações.

7.2. Constituem obrigações da empresa beneficiária da Ata, além das discriminadas no Edital do Pregão Eletrônico TRE-GO nº 54/2019 e seus anexos:

7.2.1. Assinar esta Ata e o Termo do Contrato, nos prazos determinados no Edital do Pregão Eletrônico TRE-GO nº 54/2019 e seus anexos;

7.2.2. Manter, durante a vigência deste instrumento, as condições de habilitação exigidas no edital certame que lhe deu origem;

7.2.3. Informar, no prazo máximo de 5 (cinco) dias úteis, quanto à aceitação ou não do fornecimento a outro órgão da Administração Pública, não participante deste registro de preços, que venha a manifestar o interesse em utilizar o presente ajuste;

7.2.4. Fornecer, sempre que solicitado, no prazo máximo de 5 (cinco) dias úteis, a contar da notificação, documentação de habilitação e qualificação cujas validades encontrem-se vencidas;

7.2.5. Manter atualizados seus dados e de seus representantes, tais como: endereços, telefones, fax, e-mail, dentre outros.

8. VALIDADE DA ATA

8.1. A validade da Ata de Registro de Preços será de 12 meses, a partir da assinatura, não podendo ser prorrogada.

9. DO CONTROLE E DAS REVISÕES DOS PREÇOS

9.1. Durante a vigência da Ata, os preços registrados serão fixos e irreajustáveis, exceto nas hipóteses devidamente comprovadas decorrentes das situações previstas nos artigos 17 a 19 do Decreto nº 7.892/2013.

9.1.1. Mesmo comprovada a ocorrência de situação prevista neste item, a Administração, se julgar conveniente, poderá optar por cancelar a Ata e iniciar outro procedimento licitatório.

10. DO CANCELAMENTO DO REGISTRO

10.1. O fornecedor beneficiário terá seu registro de preços cancelado na Ata, por intermédio de processo administrativo específico, assegurado o contraditório e a ampla defesa, nas seguintes hipóteses:

10.1.1. A pedido, quando:

10.1.1.1. Comprovar estar impossibilitado de cumprir as exigências da Ata, por ocorrência de casos fortuitos ou de força maior devidamente comprovados;

10.1.1.2. O seu preço registrado se tornar, comprovadamente, inexequível em função da elevação dos preços de mercado, dos insumos que compõem o custo das aquisições/contratações, desde que a comunicação por parte do fornecedor beneficiário ocorra antes do pedido de fornecimento por parte do TRE-GO.

10.1.2. Por iniciativa do TRE-GO, quando:

10.1.2.1. Não aceitar reduzir o preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

10.1.2.2. Perder quaisquer das condições de habilitação exigidas no processo licitatório;

10.1.2.3. Por razões de interesse público devidamente motivadas e justificadas;

10.1.2.4. Não cumprir as obrigações decorrentes da Ata de Registro de Preços;

10.1.2.5. Recusar-se a assinar o termo de contrato decorrente desta Ata de Registro de Preços, ou retirar/receber as respectivas notas de empenho;

10.1.2.6. Caracterizada qualquer hipótese de inexecução total ou parcial das condições estabelecidas na Ata de Registro de Preços ou nos pedidos dela decorrentes;

10.1.2.7. Sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da Lei nº 8.666, de 1993, ou no art. 7º da Lei nº 10.520, de 2002;

10.1.2.8. Houver atraso injustificado na prestação dos serviços contratados, bem como a sua paralisação sem justa causa e prévia comunicação ao TRE-GO;

10.1.2.9. Verificada qualquer uma das hipóteses acima, concluído o respectivo processo e após garantido o contraditório e a ampla defesa, sem prejuízo das sanções eventualmente cabíveis, o TRE-GO formalizará o cancelamento do registro correspondente e informará ao fornecedor beneficiário e aos demais a nova ordem de registro.

10.2. A Ata de Registro de Preço, decorrente desta licitação, será cancelada automaticamente:

10.2.1. Por extinção da totalidade do seu objeto;

10.2.2. Quando não restarem fornecedores registrados.

11. DAS PENALIDADES

11.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital.

11.2. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 5º, inciso X, do Decreto nº 7.892/2013), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 6º, § 1º, do Decreto nº 7.892/2013).

11.3. O órgão participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no art. 20 do Decreto nº 7.892/2013, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

12. DAS DISPOSIÇÕES GERAIS

12.1. As condições gerais, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no edital do Pregão TRE-GO nº 54/2019 e seus anexos.

12.2. É vedado efetuar acréscimos nos quantitativos fixados nesta ata de registro de preços, inclusive o acréscimo de que trata o § 1º do artigo 65 da Lei nº 8.666/1993.

12.3. Esta Ata não obriga o TRE-GO a firmarem contratações com o FORNECEDOR, podendo ocorrer licitações específicas para os produtos registrados, observada a legislação pertinente, sendo assegurada preferência de fornecimento ao detentor do registro em igualdade de condições.

12.4. A empresa registrada nesta ata declara estar ciente de suas obrigações para com o TRE-GO, nos termos do Edital do Pregão Eletrônico nº 54/2019 e seus anexos, que passam a fazer parte da presente ata e a reger as relações entre as partes, para todos os fins, independentemente de transcrição.

12.5. A ata de realização da sessão pública do pregão, contendo a relação dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao do licitante vencedor do certame, será anexada a esta Ata de Registro de Preços, nos termos do artigo 11, §4º do Decreto nº 7.892/2013.

Para firmeza e validade do pactuado, a presente Ata foi lavrada em 2 (duas) vias de igual teor e forma para todos os fins de direto, que, depois de lidas e achada em ordem, vão assinadas pelas partes.

WILSON GAMBOGE JUNIOR:79930506187

Assinado de forma digital por WILSON GAMBOGE JUNIOR:79930506187
DN: c=BR, o=ICP-Brasil, ou=Autoridade Certificadora Raiz Brasileira v2, ou=AC SOLUTI, ou=AC SOLUTI Multipla, ou=Certificado PF A3, cn=WILSON GAMBOGE JUNIOR:79930506187
Dados: 2019.11.19 11:01:35 -03'00'

WILSON GAMBOGE JÚNIOR
Diretor Geral do TRE/GO

ANDRE LUIZ ALVES DE OLIVEIRA:70559040130

Assinado de forma digital por ANDRE LUIZ ALVES DE OLIVEIRA:70559040130
Dados: 2019.11.19 17:41:41 -03'00'

ANDRÉ LUIZ ALVES DE OLIVEIRA
Sócio Administrador da empresa ARVVO TECNOL., CONSUL. E SERV. LTDA

Testemunhas:

MAGDA DA CONCEICAO GONCALVES:5069742

Assinado de forma digital por MAGDA DA CONCEICAO GONCALVES:5069742
DN: c=BR, o=ICP-Brasil, ou=Autoridade Certificadora da Justica - AC-JUS, ou=Cert-JUS Institucional - A3, ou=18799897000120, ou=Tribunal Regional Eleitoral Goias - TRE-GO, ou=SERVIDOR, cn=MAGDA DA CONCEICAO GONCALVES:5069742
Dados: 2019.11.19 19:21:15 -03'00'

MARCILIO ZACCARELLI BERSANETI:5062748

Assinado de forma digital por MARCILIO ZACCARELLI BERSANETI:5062748
DN: c=BR, o=ICP-Brasil, ou=Autoridade Certificadora da Justica - AC-JUS, ou=Cert-JUS Institucional - A3, ou=37622727000110, ou=Tribunal Regional Eleitoral de Goias-TRE-GO, ou=Servidor, cn=MARCILIO ZACCARELLI BERSANETI:5062748
Dados: 2019.11.19 19:46:07 -03'00'

ANEXO I
TERMO DE REFERÊNCIA

1. OBJETIVO

Registro de preços para eventual aquisição de solução de Tecnologia da Informação para Segurança e Conectividade da Rede de Dados, visando a atualização e a manutenção da infraestrutura de comunicação de dados entre os usuários e os serviços de TI utilizados no TRE-GO.

2. OBJETO

Aquisição de solução de Tecnologia da Informação para Segurança e Conectividade da Rede de Dados do TRE-GO e das Zonas Eleitorais, visando a atualização e a manutenção da infraestrutura de comunicação de dados entre os usuários e os serviços de TI utilizados no TRE-GO.

Lote 01		
Item	**Descrição**	**Quantidade**
1	Switch gerenciável de borda com 48 portas.	32 unidades
2	Switch gerenciável core.	4 unidades
3	Transceiver 1000Base-T.	40 unidades
4	Transceiver 10GBase-SR.	230 unidades
5	Software para gerenciamento de redes.	1 unidade
6	**Serviços de instalação e configuração dos equipamentos.**	1 unidade

Lote 02		
Item	**Descrição**	**Quantidade**
7	Roteador Firewall/Gateway.	2 unidades
8	**Upgrade de licença de software de gerencia.**	1 unidade
9	**Serviços de instalação e configuração dos equipamentos.**	1 unidade

Item	**Descrição**	**Quantidade**
10	Switch gerenciável com 24 portas.	100 unidades

3. JUSTIFICATIVA/MOTIVAÇÃO/RESULTADOS ESPERADOS

3.1 – Motivação/Justificativas:

Id	OBJETO	JUSTIFICATIVAS
1	Lote 1 - Item 1 - Switch gerenciável de borda com 48 portas	Pretende-se adquirir switches gerenciáveis com portas de velocidades superiores de conexão a 10Gbps com o Datacenter, para melhorar a performance dos sistemas e serviços que acessam dados na rede interna e na internet, em substituição aos atuais switches gerenciáveis com portas 1Gbps.
2	Lote 1 - Item 2 - Switch gerenciável core	Com a implantação de switches gerenciáveis de borda com velocidades de 10Gbps, torna-se obrigatória a aquisição de Switches gerenciáveis do tipo Core para que a conexão seja estabelecida, de ponta a ponta, na velocidade pretendida. Ressalto que parte destes switches será utilizada para implantar o Core de rede redundante, com conexão ao Datacenter do Anexo II.
3	Lote 1 – Item 3 - Transceiver 1000Base-T.	Dispositivo necessário ao funcionamento dos equipamentos descritos nos itens 1 e 2 do Lote 1.
4	Lote 1 – Item 4 - Transceiver 10GBase-SR.	Dispositivo necessário ao funcionamento dos equipamentos descritos nos itens 1 e 2 do Lote 1.
5	**Lote 1 – Item 5 - Software para gerenciamento de redes.**	Software necessário para gerência (configuração e manutenção) e monitoramento dos equipamentos descritos nos itens 1 e 2 do Lote 1.
6	**Lote 1 – Item 6 - Serviços de instalação e configuração dos equipamentos e software de gerência.**	Serviços necessários para a implementeção dos itens 1 a 4 do Lote 1.
7	Lote 2 - Item 7 - Roteador Firewall/Gateway.	Pretendemos substituir os atuais equipamentos de rede, da marca SonicWall, com função de Firewall/Gateway interno, por não terem mais garantia e por estarem próximos de serem descontinuados pelo fabricante, o que não nos permite contratar os serviços de garantia e de suporte. Outros aspectos são a padronização, pois 90% do parque atual é da marca Checkpoint e, a compatibilidade entre os equipamentos da plataforma de segurança e o software de gerenciamento desta solução. Trata-se de solução crítica e complexa, que define centenas de protocolos de rede e funcionalidades que precisam coexistir em perfeita compatibiliade e por se tratar de equipamentos que compõem o cerne da rede de computadores da JE-GO, não podem existir lacunas nos limites de responsabilides entre multiplos fabricantes ou revendas associados a essa solução. O modelo adequado para aquisição para atender esta demanda é o Checkpoint Gateway 5600.
8	**Lote 2 - Item 8 - Upgrade de licença de software de gerencia.**	Serviço necessário para gerenciar os antigos e os novos equipamentos da solução de segurança.

9	**Lote 2 - Item 9 - Serviços de instalação e configuração dos equipamentos.**	Serviços necessários para a implementeção do item 7 do Lote 2.
10	Item 10 - Switch gerenciável com 24 portas.	Todas as 92 Zonas Eleitorais contam com pelo menos 01 Switch não gerenciável de 16 portas com velocidade de 100Mbps, o que proporciona menor performance e menor possibilidade de ampliação do parque de ativos de rede, como computadores, firewall/roteador, impressoras e câmeras IP. Temos em andamento um procedimento de contratação de novos links de dados com velocidades superiores, o que demanda equipamentos de rede de porte maior e que suportem velocidades maiores. Portanto pretendemos atualizar todos os atuais switches por novos que suportem as novas demandas, como por exemplo a Video Conferência, e, que permitam melhor gerência e suporte com aumento da disponibilidade e qualidade das conexões.

3.2 – Alinhamento com as necessidades de negócio:

Função	Necessidade de Negócio
Possibilitar acesso aos serviços de TI.	Garantir a disponibilidade dos serviços de TI.

3.3 – Benefícios esperados:

Tipo	Benefício
Eficiência	Tráfego de dados pela rede com maior velocidade e segurança.

3.4 - Resultados a serem alcançados:

Id	Resultados
1	Aumetar a performance da rede de forma adequada ao novo Backbone secundário.
2	Implementar maior segurança na rede de dados.
3	Adequar a infraestrutura de rede às novas demandas e tecnologias a serem implantadas.

4. ALINHAMENTO ESTRATÉGICO

Esta ação está em consonância com o Planejamento Estratégico 2014/2015 da Justiça Eleitoral de Goiás, mais especificamente buscando atender ao objetivo estratégico 12, “Garantir a infraestrutura apropriada às atividades institucionais”, meta, “Prover e gerir recursos físicos (mobiliário e imobiliário) e tecnológico (equipamentos, redes, sistemas e comunicações) a fim de garantir a prestação de serviços de qualidade e condições de trabalho, com saúde e segurança.”.

5. FONTE DE RECURSOS

Para execução desta ação entendemos, s.m.j., que os recursos financeiros deverão ser provenientes da verba destinada para Aquisição de Equipamentos de Informática da programação Orçamentária de 2019/2020.

6. ESTIMATIVA DE PREÇOS

As planilhas de cálculo para estimativa de preços e os orçamentos seguem no Anexo I deste Termo de Referência.

7. ESPECIFICAÇÕES TÉCNICAS

7.1. Lote 1 – Item 1 - Switch gerenciável de borda com 48 portas.

7.1.1. CARACTERÍSTICAS GERAIS:

7.1.1.1. Equipamento tipo comutador gigabit ethernet com capacidade de operação em camada 3 do modelo OSI;

7.1.1.2. Deve ser fornecido com 48 (quarenta e oito) portas 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45;

7.1.1.3. Deve ser fornecido com 2 slots para conexão de transceivers SFP/SFP+ para fibras ópticas multimodo e monomodo com velocidade de 1GbE e 10GbE. Estas portas devem ser de uso simultâneo com as portas 1000Base-T e não serão aceitas interfaces do tipo combo com qualquer uma das 48 portas 1000Base-T exigidas;

7.1.1.4. Deve possuir 50 portas ethernet ativas simultaneamente, não incluindo interfaces de empilhamento;

7.1.1.5. Deve permitir a criação de links agrupados virtualmente (link aggregation) utilizando portas de diferentes switches da pilha;

7.1.1.6. Deve possuir porta de console para total gerenciamento local, com conector RS-232, RJ-45 ou USB;

7.1.1.7. Deve possuir capacidade de vazão de, pelo menos, 120 Mpps;

7.1.1.8. Deve permitir o espelhamento do tráfego de uma porta (port mirroring) para outra porta do mesmo switch ou para uma porta de outro switch que estiver na rede.

7.1.1.9. Deve possuir Jumbo Frame de pelo menos 9000 bytes;

7.1.1.10. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, permitindo a criação de no mínimo 1000 VLANs com IDs entre 1 e 4000;

7.1.1.11. Deve implementar roteamento IP (Layer 3) com pelo menos 4 interfaces roteáveis, permitindo a criação de pequenos backbones;

7.1.1.12. Deve permitir a criação de links agrupados virtualmente (link aggregation);

7.1.1.13. Permitir a descoberta de outros dispositivos na rede de forma automática através do protocolo LLDP (IEEE 802.1AB) ou semelhantes;

7.1.1.14. Deve possuir IGMP snooping para controle de tráfego de multicast;

7.1.1.15. Deve suportar Multicast VLAN, de forma que o tráfego Multicast da rede seja isolado em uma VLAN diferente das demais;

7.1.1.16. Deve implementar MLD v1 e v2;

7.1.1.17. Deve identificar automaticamente portas em que telefones IP estejam conectados e associá-las automaticamente a VLAN de voz;

7.1.1.18. Deve implementar Spanning Tree por VLAN e conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree) com filtros BPDU. Deve implementar pelo menos 15 instâncias de Multiple Spanning Tree;

7.1.1.19. Deve possuir priorização de pacotes (QoS) com 7 (sete) filas de prioridade por porta. Deve implementar a classificação de pacotes com base em regras de ACL;

7.1.1.20. Deve possuir autenticação IEEE 802.1x com assinalamento de VLAN por usuário e Guest VLAN para usuários não autenticados. Para usuários sem cliente IEEE 802.1x instalado, deve possuir um portal Web interno ao equipamento para autenticação;

7.1.1.21. Deve possuir autenticação IEEE 802.1x de múltiplos usuários por porta para o caso de uplinks com switches não gerenciáveis. Apenas o tráfego dos usuários que se autenticarem será permitido;

7.1.1.22. Deve implementar criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes a senha;

7.1.1.23. Deve permitir configurar quantos endereços MAC podem ser aprendidos em uma porta e permitir configurar qual ação será tomada quando esta regra for quebrada: alertar ou desativar a porta;

7.1.1.24. Deve permitir a criação de listas de acesso (ACLs), internamente ao equipamento, baseadas em endereço IP de origem, endereço IP de destino, portas TCP e UDP, campo DSCP, campo ToS e dia e hora. Deve ser possível habilitar o log da ACL;

7.1.1.25. Deve implementar Ipv6;

7.1.1.26. Deve permitir a configuração de DHCP Server e DHCP Relay com suporte a múltiplas VLANs simultaneamente;

7.1.1.27. Deve possuir DHCP Snooping para eliminação de falsos servidores DHCP;

7.1.1.28. Deve possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC, de forma a evitar ataques na rede;

7.1.1.29. Deve possuir o protocolo “Network Time Protocol” (NTP) ou “Simple Network Time Protocol” (SNTP) para a sincronização do relógio com outros dispositivos de rede, garantindo a alta efetividade e segurança na troca de mensagens com os servidores de tempo;

7.1.1.30. Deve possuir interface USB para manipulação de arquivos com firmware ou configuração localmente;

7.1.1.31. Deve permitir configuração/administração remota através de SSH e SNMPv3;

7.1.1.32. Deve permitir a criação de três níveis de administração e configuração do switch. Deve permitir a autenticação de usuário de gerência em servidor RADIUS e TACACS, TACACS+ ou similar;

7.1.1.33. Deve implementar tecnologia que colete amostras do fluxo de tráfego (flows) para fornecimento de estatísticas e monitoramento da rede através dos protocolos Netflow, IPFIX ou sFlow;

7.1.1.34. Deve implementar o mecanismo mudança de autorização dinâmica para 802.1x, conhecido como RADIUS CoA (Change of Authorization);

7.1.1.35. Deve permitir o envio de mensagens geradas pelo sistema em servidor externo (syslog), indicando a hora exata do acontecimento;

7.1.1.36. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136;

7.1.1.37. Deve suportar fonte de alimentação redundante;

7.1.1.38. Gabinete padrão para montagem em rack de 19", com altura máxima de 1U, incluindo todos os acessórios para o perfeito funcionamento;

7.1.2. EMPILHAMENTO:

7.1.2.1. Deve permitir o empilhamento de, pelo menos, 4 (quatro) unidades;

7.1.2.2. Deve possuir interfaces de empilhamento com as seguintes características:

7.1.2.2.1. Podem ser fixas e/ou em modulo adicionado ao comutador;

7.1.2.2.2. Devem ser fornecidas, no mínimo, 2 (duas) interfaces;

7.1.2.2.3. Todas as interfaces devem ser iguais quanto à velocidade e quanto aos meios físicos de conexão;

7.1.2.2.4. Devem ser separadas das interfaces fornecidas para acesso ou para uplink;

7.1.2.2.5. Devem suportar, somadas, no mínimo, o tráfego de 80Gbps, podendo ser considerado o tráfego full-duplex. Este requisito deve ser alcançado com o uso de, no máximo, 4(quatro) interfaces;

7.1.2.2.6. Devem ser fornecidas com todos os componentes necessários para o pleno funcionamento da pilha;

7.1.2.2.7. Cada unidade deve vir acompanhada de, pelo menos, 1 (um) cabo de, no mínimo, 0,5m de comprimento para o empilhamento. Caso o modelo fornecido exija mais de 2 (duas) interfaces para o atendimento dos requisitos mínimos de tráfego do empilhamnto, devem ser fornecidos 2 (dois) cabos por unidade de comutador;

7.1.3. Visando atender à padronização que imponha compatibilidade técnica e de desempenho, os itens constantes deste lote deverão ser do mesmo fabricante.

7.2. Lote 1 – Item 2 - Switch gerenciável core.

7.2.1. CARACTERÍSTICAS GERAIS:

7.2.1.1. Equipamento com operação na camada 3 do modelo OSI (Layer 3);

7.2.1.2. O equipamento deve possuir instalada, no mínimo, a seguinte configuração de portas:

7.2.1.2.1. Deve possuir, no mínimo, 4 (quatro) portas do padrão QSFP+ ou, no mínimo, 2 (duas) portas QSFP28;

7.2.1.2.2. Deve permitir a utilização de cabos breakout nas portas QSFP+ ou QSFP28 para conversão de uma determinada interface em quatro conexões de 10GbE (para portas QSFP+) ou em quatro conexões de 25GbE (para portas QSFP28);

7.2.1.2.3. Deve possuir, no mínimo, 48 (quarenta e oito) interfaces SFP+ para conexão de fibras ópticas monomodo ou multimodo com velocidades de 1 e 10 Gigabit Ethernet;

7.2.1.3. O switch deve implementar non-blocking wire speed em todas as portas;

7.2.1.4. Deve acompanhar 2 (dois) cabos de conexão direta em 40GbE, caso seja atendido com portas QSFP+, ou 1 (um) cabo de conexão direta em 100GbE, caso seja atendido com portas QSFP28. Os cabos devem ter, no mínimo, 1 (um) metro;

7.2.1.5. Deve possuir gabinete de no máximo 01 (um) RU (rack unit) e permitir instalação em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;

7.2.1.6. Possuir porta de console para ligação direta, de terminal RS-232 ou RJ-45 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

7.2.1.7. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implantação de todas as funcionalidades descritas nesta especificação;

7.2.1.8. Permitir o encaminhamento de “jumbo frames” em todas as portas (pacotes de 9000 bytes);

7.2.1.9. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática. Deve incluir fonte de alimentação redundante. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136;

7.2.1.10. Deverá ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas;

7.2.1.11. Possuir LEDs para a indicação do status das portas e atividade;

7.2.1.12. A ventilação do equipamento deverá seguir o fluxo onde o ar entra através das portas e com exaustão através das fontes;

7.2.1.13. Possuir capacidade para pelo menos 82.000 (oitenta e dois mil) endereços MAC na tabela de comutação;

7.2.1.14. Possuir backplane de, no mínimo, 1,2 Tbps (Terabits por segundo);

7.2.1.15. O equipamento deve ter capacidade mínima de encaminhamento de 900 Mpps (Milhões de pacotes por segundo);

7.2.2. GERENCIAMENTO:

7.2.2.1. Implementar os padrões abertos de gerência de rede SNMP (v1, v2 e v3), incluindo a geração de traps;

7.2.2.2. Suportar SNMP sobre IPv6;

7.2.2.3. Possuir suporte a MIB II, conforme RFC 1213;

7.2.2.4. Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento;

7.2.2.5. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;

7.2.2.6. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

7.2.2.7. Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;

7.2.2.8. Ser configurável e gerenciável via CLI (command line interface), Telnet e SSH;

7.2.2.9. Permitir que a configuração seja realizada através de terminal assíncrono;

7.2.2.10. Permitir a gravação de log externo (syslog);

7.2.2.11. Possuir 1 (uma) porta 10/100/1000BaseT, com conector RJ-45, exclusivamente para gerência do equipamento. Esta porta será conectada na rede de gerência e o switch deverá permitir a configuração de endereço IP próprio para gerenciamento;

7.2.2.12. O equipamento deve permitir sua configuração através de NETCONF;

7.2.2.13. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace e log de eventos;

7.2.3. FACILIDADES:

7.2.3.1. Permitir a agregação de, no mínimo, 08 (oito) portas segundo o padrão IEEE 802.3ad;

7.2.3.2. Deve permitir a criação de links de agregação entre interfaces de dois equipamentos separados e idênticos, especificados nesta seção do edital, e pelo menos duas interfaces de

um terceiro dispositivo que suporte 802.3ad, este que tratará o link redundante de forma transparente como se estivesse conectado a um único equipamento. Esta funcionalidade também é conhecida como Multi-Chassis Link Agregation, MultiChassis Etherchannel, Multi-Switch Link Aggregation (M-LAG) ou Virtual PortChannel. Alternativamente o equipamento deve permitir o empilhamento de, no mínimo, 8 unidades de mesmo modelo que permita a gerência como uma única entidade lógica;

7.2.3.3. Implementar VLANs compatíveis com o padrão IEEE 802.1q. Deve implementar, no mínimo, 4.000 (quatro mil) VLANs simultaneamente;

7.2.3.4. Permitir o espelhamento do tráfego total de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch, localizada em outro switch do mesmo tipo conectado à mesma rede local, ou mesmo, localizada em um switch do mesmo tipo com endereço IP remoto;

7.2.3.5. Permitir a virtualização das tabelas de roteamento em camada 3 através de VRFs "Virtual Routing and Forwarding" ou VRF-Lite;

7.2.3.6. Implementar o protocolo NTP (Network Time Protocol);

7.2.3.7. Deve suportar a autenticação dos servidores NTP;

7.2.3.8. Deve suportar o protocolo IPv6;

7.2.3.9. Deve implementar DHCP Relay ou UDP Helper;

7.2.3.10. Deve implementar Virtual Extensible LAN (VXLAN);

7.2.4. ROTEAMENTO:

7.2.4.1. Implementar roteamento estático IPv4 e IPv6;

7.2.4.2. Implementar protocolo de roteamento dinâmico OSPF;

7.2.4.3. Implementar protocolo de roteamento BGPv4;

7.2.4.4. Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway;

7.2.4.5. Implementar simultaneamente, no mínimo, 255 (duzentos e cinquenta e cinco) grupos do VRRP ou do mecanismo similar de redundância de gateway;

7.2.4.6. Implementar roteamento baseado em política (Policy-based Routing);

7.2.4.7. Implementar Equal-Cost Multipath (ECMP) para permitir a criação de múltiplas rotas para o mesmo destino;

7.2.5. SEGURANÇA:

7.2.5.1. Implementar mecanismo de AAA (Authentication, Authorization e Accounting) para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+/HWTACACS ou RADIUS;

7.2.5.2. Deve permitir a criação de listas de acesso (ACLs), internamente ao equipamento, baseadas em endereço IP de origem, endereço IP de destino, portas TCP e UDP;

7.2.5.3. Deve implementar filtragem de pacotes IPv6 através de Access Control List (ACL);

7.2.5.4. Deve ser possível habilitar o log das ACLs IPv4;

7.2.5.5. Possibilitar a autenticação da sessão SSH através de certificado digital;

7.2.5.6. Implementar funcionalidade para controle do volume de tráfego unicast, multicast e broadcast de uma interface;

7.2.5.7. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

7.2.5.8. Implementar mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques no ambiente nível 2;

7.2.5.9. Implementar mecanismo para suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em uma determinada porta do switch;

7.2.6. PADRÕES:

7.2.6.1. Implementar padrão IEEE 802.1d (Spanning Tree Protocol);

7.2.6.2. Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);

7.2.6.3. Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 50 (cinquenta) instâncias simultâneas do protocolo Spanning-Tree;

7.2.6.4. Implementar padrão IEEE 802.1Q (Vlan Frame Tagging);

7.2.6.5. Implementar padrão IEEE 802.1p (Class of Service);

7.2.6.6. Implementar padrão IEEE 802.3ad (LACP);

7.2.6.7. Permitir a descoberta de outros dispositivos na rede de forma automática através do protocolo LLDP (IEEE 802.1AB) ou semelhantes;

7.2.7. MULTICAST:

7.2.7.1. Implementar mecanismo de controle de multicast através de IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376);

7.2.7.2. Implementar o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;

7.2.7.3. Implementar roteamento multicast através do protocolo PIM (Protocol Independent Multicast) no modo "sparse-mode" conforme RFC 3569;

7.2.8. QUALIDADE DE SERVIÇO (QoS):

7.2.8.1. Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;

7.2.8.2. Deve permitir a classificação do tráfego em classes utilizando como base os seguintes métodos: Listas de controle de acessos (ACL), campo CoS (Class of Service), DSCP (Differentiated Services Code Point) e IP Precedence;

7.2.8.3. Uma vez classificado o tráfego, o equipamento deve marcar os seguintes campos: Class of Service (CoS), Differentiated Services Code Point (DSCP) e IP Precedence;

7.2.8.4. O equipamento deve implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);

7.2.8.5. Deve suportar o mecanismo Explicit Congestion Notification (ECN);

7.2.8.6. Deve suportar Priority Flow Control (PFC) conforme o padrão IEEE 802.1Qbb.

7.2.9. Visando atender à padronização que imponha compatibilidade técnica e de desempenho, os itens constantes deste lote deverão ser do mesmo fabricante.

7.3. Lote 1 – Item 3 - Transceiver 1000Base-T

7.3.1. CARACTERÍSTICAS GERAIS:

7.3.1.1. Transceiver SFP para conexão de cabos de par trançado;

7.3.1.2. Deve ser compatível com o padrão 1000Base-T;

7.3.1.3. Deve possuir conector RJ-45;

7.3.1.4. Velocidade de 1GbE;

7.3.2. Deve ser do mesmo fabricante, homologado e compatível com os switchs (comutadores) descritos no item 2 do Lote 01.

7.4. Lote 1 – Item 4 - Transceiver 10GBase-SR

7.4.1. CARACTERÍSTICAS GERAIS:

7.4.1.1. Transceiver SFP+ para conexão de fibras ópticas multimodo;

7.4.1.2. Deve ser compatível com o padrão 10GBase-SR para fibras ópticas OM4;

7.4.1.3. Deve possuir conector LC;

7.4.1.4. Deve possuir velocidade de 10GbE;

7.4.2. Deve ser do mesmo fabricante, homologado e compatível com os switchs (comutadores) descritos nos itens 1 e 2 do Lote 01.

7.5. Lote 1 – Item 5 - Software para gerenciamento de redes.

7.5.1. Características Gerais:

7.5.1.1. Deve ser compatível e do mesmo fabricante dos itens 1 e 2 do Lote 01;

7.5.1.2. Deve ser licenciado para gerenciar e monitorar, no mínimo, a quantidade de equipamentos previstas no Lote 1;

7.5.1.3. Deve ter todos os componentes necessários (Exemplo: banco de dados relacional) para o seu pleno funcionamento com licenças inclusas;

7.5.1.4. Deve implementar controle de acesso baseado em privilégios, permitindo a criação de grupos de operadores com acesso com limitação de quais equipamentos e quais serviços da plataforma poderão ser usados;

7.5.1.5. Deve permitir a autenticação dos operadores através de base local e através de RADIUS e/ou LDAP;

7.5.1.6. Deve executar o registro das ações executadas pelos operadores nos equipamentos gerenciados, para efeito de auditoria;

7.5.1.7. Deve suportar a utilização de sistemas de banco de dados como base de armazenamento dos dados;

7.5.1.8. Deve permitir sua operação utilizando Web Browser convencional ou através de cliente instalado em sistemas operacionais Windows;

7.5.1.9. Deve permitir a instalação e utilização em sistemas operacionais Windows Server ou Linux Server;

7.5.1.10. Deve suportar sua execução em servidores Windows ou Linux virtualizados em VMWare 5.5 ou superior;

7.5.1.11. Deve permitir a descoberta de elementos de rede através da faixa de endereços IP;

7.5.1.12. Deve permitir a configuração, monitoramento, adição e gerência de um dispositivo e também de um grupo de dispositivos;

7.5.1.13. Deve gerar o mapa e permitir a visualização da topologia da rede;

7.5.1.14. Deve permitir a customização dos mapas de topologia da rede;

7.5.1.15. Deve permitir, através da interface gráfica, ativar cliente ssh para acesso à interface CLI do equipamento;

7.5.1.16. Deve mostrar as estatísticas de utilização do equipamento contemplando no mínimo utilização de memória e de CPU;

7.5.1.17. Deve permitir a visualização de informações dos dispositivos e componentes instalados, trazendo informações como fabricante, modelo, número de série, versão de hardware e software e outras informações que sejam disponibilizadas pelo equipamento gerenciado.

7.5.1.18. Deve permitir atualizar o software do dispositivo gerenciado;

7.5.1.19. Deve permitir o agendamento de backups da configuração dos dispositivos gerenciados;

7.5.1.20. Deve permitir a criação de relatórios de histórico de backups e atualizações de software;

7.5.1.21. Deve possuir capacidade de gerar alarmes a partir de traps SNMP ou mensagens Syslog;

7.5.1.22. Deve possuir painel único de visualização dos alarmes em que se possa verificar detalhes específicos de um alarme;

7.5.1.23. Deve possuir a capacidade de enviar e-mails para um administrador em caso de algum evento especificado;

7.5.1.24. Deve possuir capacidade de monitorar o desempenho dos equipamentos gerenciados;

7.5.1.25. Deve possuir capacidade de monitorar a utilização de CPU, utilização de Memória, tempo de resposta e disponibilidade;

7.5.1.26. Deve permitir a visualização em tempo real de itens monitorados;

7.5.1.27. Deve permitir a criação de ACLs;

7.5.1.28. Deve permitir a visualização e configuração de listas de controle de acesso (ACL) nos equipamentos gerenciados compatíveis;

7.5.1.29. Deve realizar a configuração e controle centralizado de VLANs, ACLs e políticas de QoS para serem aplicadas nos switches gerenciados;

7.5.1.30. Deve possuir capacidade de visualizar os dispositivos que fazem parte de uma VLAN no mapa de topologia;

7.5.1.31. Deve possuir capacidade de gerar relatórios de:

7.5.1.31.1. Ativos de Rede;

7.5.1.31.2. Configuração e alterações de configuração;

7.5.1.31.3. Estado dos dispositivos e Links;

7.5.1.31.4. Eventos e Alarmes;

7.5.1.32. A Contratada deverá instalar e configurar o software para gerenciamento de redes e todos os componentes necessários para o seu pleno funcionamento no ambiente do Contratante de forma presencial. Os equipamentos dos itens 01 e 02 do Lote 01 devem ser adicionados no sistema para sua correta gerência e monitoramento.

7.6. Lote 1 – Item 6 - Serviços de instalação e configuração dos equipamentos.

7.6.1. Informações gerais:

7.6.1.1. Este item descreve os serviços para os itens 1 e 2 do Lote 01 deste Termo de Referência;

7.6.1.2. Este item consiste na prestação de serviços técnicos especializados para instalação e configuração, com transferência de tecnologia, dos equipamentos descritos nos itens de 01 a 02 deste Termo de Referência;

7.6.1.3. Estes serviços deverão ser executados por profissionais especializados e indicados pela Contratada, com qualificação e certificação em LAN Switch, especificamente dos produtos a serem entregues em conformidade com o especificado nos itens 1 e 2;

7.6.1.4. A transferência de tecnologia deverá ser realizada para, pelo menos, 2 técnicos da SESRE;

7.6.1.5. Os serviços devem ser obrigatoriamente prestados pela mesma empresa contratada para fornecer os esquipamentos;

7.6.1.6. A Contratada deverá apresentar um Plano de Gerenciamento de Projetos – PGP que deverá conter, no mínimo:

7.6.1.6.1. As atividades que serão executadas;

7.6.1.6.2. Os produtos que serão gerados;

7.6.1.6.3. Proposta de cronograma para a execução do objeto;

7.6.1.6.4. Os possíveis riscos;

7.6.1.6.5. Outras informações consideradas importantes para a aprovação da solicitação de serviço pela CONTRATANTE;

7.6.1.7. Uma vez de posse do PGP, o CONTRATANTE deverá analisar todas as cláusulas e aprová-lo ou não. Este documento deverá ser ajustado de forma a obedecer aos requisitos de ambas as partes;

7.6.1.8. Todos os serviços deverão ser realizados em horário comercial – das 08:00 às 18:00hs;

7.6.1.9. Responsabilidades do Contratante:

7.6.1.9.1. É de inteira responsabilidade do Contratante a disponibilização de rack para a instalação dos equipamentos;

7.6.1.9.2. É de inteira responsabilidade do Contratante a disponibilização de pontos elétricos para a energização de todos os equipamentos;

7.6.1.9.3. É de inteira responsabilidade do Contratante a disponibilização e a conectorização de todos os cabos necessários para ligação dos equipamentos à rede local (LAN) do contratante;

7.6.2. Escopo do serviço:

7.6.2.1. Configuração dos equipamentos novos nos locais designados pela contratante;

7.6.2.2. Atualização de firmware para a última versão estável disponibilizada pelo fabricante dos equipamentos;

7.6.2.3. Devem ser mapeadas todas as VLANs existentes na infraestrutura da contratante. Após o mapeamento deve ser realizado trabalho crítico sobre as VLANs existentes com a finalidade de melhorias e sugestões conforme as melhores práticas e recomendações de mercado;

7.6.2.4. Devem ser criadas VLANs exclusivas para funcionários, usuários visitantes, impressoras, voz, vídeo, CFTV, controle de acesso, gerenciamento dos equipamentos,

vídeoconferência, TI, desenvolvimento de sistemas, servidores em produção, laboratório, testes, DMZ e mais as VLANs dos Departamentos que somados são 20 VLANs. Outras VLANs podem ser necessárias, a critério do Contratante;

7.6.2.5. Devem ser criadas políticas de acesso entre VLANs, através de listas de controle de acesso (ACL), capaz de garantir que somente o tráfego permitido extrapolará o perímetro das VLANs, aumentando o nível de segurança na rede;

7.6.2.6. Devem ser aplicados recursos de segurança para prevenir ataques contra a infraestrutura, incluindo DHCP snooping, dynamics ARP inspection (DAU) e bloqueio de quantidade de endereços MACs aprendidos por porta;

7.6.2.7. Deverá ser configurado o protocolo spanning tree (e suas derivações/melhorias) para prevenir qualquer problema com loop na rede. Deve ser elegido o equipamento que será configurado como bridge raiz (e este deverá ter a menor prioridade possível) e as portas dos equipamentos de acesso deverão estar configuradas para permitir a conexão rápida de dispositivos, de modo a não prejudicar a adição de novos dispositivos na rede. Devem ser configurados também as opções loop guard, root guard, bpdu guard e bpdu filter;

7.6.2.8. Para comunicação entre os equipamentos de borda e o CORE devem ser configuradas 16 link aggregation distintas;

7.6.2.9. Todos os equipamentos devem ser configurados para permitir o gerenciamento através do protocolo SNMPv3 com autenticação e deve permitir o acesso via terminal ssh. O acesso via telnet deve ser desabilitado;

7.6.2.10. Deve ser entregue relatório contendo todo o serviço realizado executado;

7.6.2.11. Deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante e acompanhada pelos técnicos da contratante;

7.6.2.12. Durante toda a implantação do projeto, o técnico da contratada deverá demonstrar aos técnicos da contratante como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados;

7.7. Lote 2 – Item 7 - Roteador Firewall/Gateway.

7.7.1. Deverá ser da Marca Check Point, Modelo 5600.

7.7.2. CARACTERÍSTICAS GERAIS:

7.7.2.1. A solução deve ser composta por 02 (dois) equipamentos Firewall/Gateway VPN, de mesma capacidade e modelo, operando em modo de alta disponibilidade (cluster);

7.7.2.2. As especificações aqui detalhadas se referem a capacidade de 01 (um) dos equipamentos;

7.7.2.3. Tamanho máximo de 1U por equipamento;

7.7.2.4. Cada appliance de segurança, deverá possuir no mínimo os seguintes throughput:

7.7.2.4.1. Throughput de 20 (vinte) Gbps para a funcionalidade de firewall;

7.7.2.4.2. Throughput de 05 (cinco) Gbps para a funcionalidade de IPS;

7.7.2.4.3. Throughput de 06 (seis) Gbps para funcionalidade de VPN com algoritmo AES-128;

7.7.2.5. Sendo que o appliance não deve sofrer degradação de performance quando as funcionalidades de Firewall, Controle de aplicação WEB e IPS tiverem habilitadas de forma simultânea, sendo que o trafego deverá ser inspecionado de modo bidirecional e a inspeção deve ser feita para toda a sessão do pacote, sem qualquer utilização de feature de bypass do pacote/sessão.

7.7.2.6. Possuir alimentação elétrica a partir de, no mínimo, 02 (duas) fontes internas independentes, redundantes e hotswap, capazes de operar entre 100 a 120VAC e entre 200 e 240VAC, por reconhecimento automático do nível de tensão;

7.7.2.7. Deve possuir 10 (dez) interfaces de rede 10/100/1000 Base-T RJ-45;

7.7.2.8. Deve possuir 04 (quatro) interfaces de rede 1000Base-F SFP;

7.7.2.9. A solução deve suportar até 04 (quatro) interfaces 10 Gigabit SFP+;

7.7.2.10. Possuir, no mínimo, 01 (uma) interface de rede 10/100/1000 Gbps dedicada para o gerenciamento, podendo ser utilizada uma das interfaces do subitem 7.6.2.7;

7.7.2.11. Possuir, no mínimo, 01 (uma) interface do tipo console ou similar;

7.7.2.12. Possuir, no mínimo, 01 (uma) interface de rede 10/100/1000 Gbps dedicada para alta disponibilidade, podendo ser utilizada uma das interfaces do subitem 7.6.2.7;

7.7.2.13. Possuir interface de gerenciamento do tipo LOM;

7.7.2.14. A solução deve possuir disco rígido de, no mínimo, 200 GB sendo ele do tipo SSD (Solid-Stade Drive);

7.7.3. CONTROLE DE POLÍTICAS DE FIREWALL:

7.7.3.1. A solução deve incluir appliance do próprio fabricante;

7.7.3.2. Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado;

7.7.3.3. O sistema operacional da solução deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance;

7.7.3.4. Deve suportar atuação como cliente NTP (Network Time Protocol) versão 1, 2, 3 e 4;

7.7.3.5. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

7.7.3.6. O hardware deve ser baseado em arquitetura aberta usando processadores Intel ou AMD a fim de manter flexibilidade e adaptação a novas ameaças sem impacto na performance;

7.7.3.7. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

7.7.3.8. A comunicação entre a solução de gerência e os appliances de segurança deverá ser criptografada, sendo que a comunicação entre eles deve ser protegida através de uma Infraestrutura de Chaves Públicas interna do próprio fabricante da Solução ofertada;

7.7.3.9. Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos;

7.7.3.10. A solução deve permitir que em caso de falha de comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária na mesma unidade física de armazenamento do sistema operacional do appliance de segurança;

7.7.3.11. A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos, permitindo a pesquisa dos mesmos em todo o log orientado aos sentidos vertical, horizontal e transversal, sendo necessário apenas a informação da string de texto no campo de pesquisa para que seja feito o filtro dos eventos NGFW de forma agregada e multidisciplinar (trazendo a trilha das diversas funcionalidades relacionadas a esta pesquisa);

7.7.3.12. As regras deverão ser construídas utilizando objetos de rede baseadas no protocolo IP. Durante a criação da regra, tais objetos deverão ser associados automaticamente às suas interfaces de rede correspondentes, sem que haja necessidade de o administrador associar, na regra, qual é a interface de rede origem da conexão, nem a interface de rede destino da conexão. Não será aceito definição de interface com a variável “any”;

7.7.3.13. Deve suportar a implementação de monitoração de links Internet, através do teste de conectividade com endereços específicos e implementar alertas em caso de quedas;

7.7.3.14. Deverá possibilitar a implementação de balanceamento de links em modos de Ativo/Ativo ou Ativo/Passivo.

7.7.3.15. Após uma queda da conexão primária, quando essa retornar deve ser possível configurar as ações como por exemplo alertas de SNMP, log, scripts customizados pelo usuário.

7.7.3.16. Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;

7.7.3.17. A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: Tokens (como SecurID), TACACS, RADIUS, certificados digitais e dispositivos biométricos

7.7.3.18. Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;

7.7.3.19. Em caso de falhas nas rotas primárias deve desviar dinamicamente o tráfego para um link secundário, roteamento com base em prioridades;

7.7.3.20. Implementar roteamento e encaminhamento baseado em políticas;

7.7.3.21. Deve implementar roteamento multicast (PIM-SM);

7.7.3.22. Possuir funcionalidade de DHCP Relay e DHCP Server;

7.7.3.23. Suporte à criação de objetos de rede, sendo que um mesmo objeto possa ser utilizado com endereço IP nas versões 4 e 6 simultaneamente a este mesmo objeto que será associado à base de regras;

7.7.3.24. Possuir base de regras singular sem separação de regras orientadas a versão de endereço IP utilizada;

7.7.3.25. Prover a otimização administrativa e lógica quando referenciado há um mesmo host com as duas versões do endereço IP sem a multiplicação de objetos e regras;

7.7.3.26. Implementar sub-interfaces ethernet lógicas;

7.7.3.27. Deve suportar os seguintes tipos de NAT:

7.7.3.27.1. Nat dinâmico (Many-to-1);

7.7.3.27.2. Nat dinâmico (Many-to-Many);

7.7.3.27.3. Nat estático (1-to-1);

7.7.3.27.4. NAT estático (Many-to-Many);

7.7.3.27.5. Nat estático bidirecional 1-to-1;

7.7.3.27.6. NAT de Origem;

7.7.3.27.7. NAT de Destino;

7.7.3.28. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

7.7.3.29. Deve implementar roteamento estático IPv4 e IPV6;

7.7.3.30. Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4;

7.7.3.31. Deve implementar roteamento dinâmico (OSPFv3) para IPv6;

7.7.3.32. Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing);

7.7.3.33. Deve suportar no mínimo as seguintes funcionalidades:

7.7.3.33.1. A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através de padrões de análise de protocolo tais como de Tipo de Protocolo ou Inspeção de SSH;

7.7.3.33.2. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

7.7.3.33.3. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

7.7.3.34. Deve ter a capacidade de inspecionar e bloquear tráfego operando nos seguintes modos: camada 2 (L2) e camada 3 (L3);

7.7.3.35. Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações;

7.7.3.36. Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações;

7.7.3.37. Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);

7.7.3.38. Na ocorrência de falhas, as conexões existentes em um firewall deverão ser mantidas pelo (s) outro (s) sem perdas destas conexões, não acarretando interrupções no tráfego da rede;

7.7.3.39. Na aplicação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas;

7.7.3.40. Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar as informações armazenadas para realizar autenticações;

7.7.3.41. Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS;

7.7.3.42. A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;

7.7.3.43. A solução não deve por "default" permitir que todas as portas TCP/UDP resultem em um estado do tipo "open" após um "scan ports";

7.7.3.44. Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;

7.7.3.45. Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;

7.7.3.46. Deverá suportar métodos de autenticação de usuário, cliente e sessão;

7.7.3.47. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando existirem múltiplos executando alterações simultaneamente;

7.7.3.48. Habilidade de realizar upgrade via SCP ou https via interface WEB;

7.7.3.49. A solução de segurança deve possuir capacidade de endereços MAC trafegados superior a 4.000 endereços;

7.7.3.50. A solução deverá disponibilizar uma ferramenta onde o fabricante disponibilize HotFixes de segurança e upgrades de versão para instalação simples e com zero-downtime;

7.7.3.51. Possuir funcionalidade de HTTP e HTTPS proxy.

7.7.4. ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA:

7.7.4.1. Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:

7.7.4.1.1. Em modo Transparente:

7.7.4.1.2. Em Layer 2;

7.7.4.1.3. Em Layer 3;

7.7.4.2. O HA deve sincronizar:

7.7.4.2.1. Todas as sessões;

7.7.4.2.2. Certificados de-criptografados;

7.7.4.2.3. Todas Associações de Segurança das VPNs;

7.7.4.2.4. Todas as assinaturas de Anti-virus, Anti-spyware, Aplicações Web 2.0 e IPS;

7.7.4.3. O HA (modo de Alta-Disponibilidade) deve possibilitar tracking de IP.

7.7.4.4. Monitoração de falha de link.

7.7.4.5. Para melhor desempenho ou em caso de crescimento da rede, a solução deve suportar mais de dois membros no cluster de NG Firewall ou NGTP;

7.7.4.6. A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

7.7.4.7. Suportar agregação de links 802.3ad sem a limitação da combinação de portas devido hardware de aceleração proprietário do fabricante;

7.7.5. VPN:

7.7.5.1. A solução deve suportar CA Interna e CA Externa de terceiros;

7.7.5.2. Solução deve suportar 3DES e AES-256 de criptografia para IKE Fase I e "Suite-B-MCG-128" "Suite-B-GCM-256" para a fase II;

7.7.5.3. Solução deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 e Grupo 20;

7.7.5.4. Solução deve suportar a integridade dos dados com MD5, SHA1, SHA-256, SHA-384 e AES-XCBC;

7.7.5.5. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

7.7.5.6. A Solução deve suportar clientless SSL VPN para acesso remoto;

7.7.5.7. Solução deve suportar VPNs baseadas em redes e VPNs através de rotas com suporte a protocolos de roteamento dinâmico;

7.7.5.8. Solução deve incluir a capacidade de estabelecer VPNs com gateways de IPs públicos dinâmicos;

7.7.5.9. Solução deve incluir compressão IP para client-to-site e VPN site-to-site;

7.7.5.10. Suportar IPSec VPN:

7.7.5.10.1. Criptografia DES, 3DES, AES128, AES256, AES-GCM-128 e AES-GCM-256;

7.7.5.10.2. Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;

7.7.5.10.3. Diffie-Hellman Group 1, Group 2 e Group 5, Group 14, Group 19, Group 20;

7.7.5.10.4. Algoritmo Internet Key Exchange (IKE) versões I e II;

7.7.5.10.5. AES 128 ou 192 e 256 (Advanced Encryption Standard);

7.7.5.11. Permitir através da Gerência centralizada a criação e utiização de certificados gerados pela PKI interna da mesma que serão disponibilizados para acessos site-to-site e client-to-site;

7.7.5.12. Deve ser capaz de estabelecer VPN utilizando a funcionalidade Link Selection através do protocolo Check Point RDP. Esta VPN será estabelecida com os equipamentos atualmente em uso na Justiça Eleitoral;

7.7.6. VPN SSL

7.7.6.1. A solução deve suportar Secure Sockets Layer versão (SSL) 3, com os seguintes algoritmos de cifra simétrica e comprimentos de chave: RC4 (128 bits), 3DES (128 e 256bits) e AES (128 e 256bits);

7.7.6.2. A solução deve possuir licenciamento para, no mínimo, 5 usuários simultâneos;

7.7.6.3. A solução deve ter a opção de impor controle de login simultâneo, bloqueando sessões simultâneas do mesmo usuário;

7.7.6.4. A solução deve possuir interface intuitiva, personalizável oferecendo aos usuários fácil acesso aos aplicativos, todos com um single-sign-on;

7.7.6.5. Permitir suporte integrado à VPN SSL client-to-site nativo ou via licenciamento adequado;

7.7.6.6. A VPN SSL deve oferecer um ambiente de trabalho seguro, criando um desktop virtual sobre o desktop normal dos usuários remotos, completamente isolado. Aplicações maliciosas e vírus presentes no desktop normal não podem afetar o desktop virtual. Todas as informações presentes do desktop virtual devem estar criptografadas;

7.7.6.7. Além de criptografar e proteger informações de sessão do usuário, a solução de VPN SSL deve permitir ao administrador configurar quais aplicações podem ser executadas durante o uso do ambiente de trabalho seguro;

7.7.6.8. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

7.7.6.9. O cliente de VPN deverá estar disponível para as seguintes plataformas:

7.7.6.9.1. Windows XP;

7.7.6.9.2. Windows 7;

7.7.6.9.3. Windows 8;

7.7.6.9.4. Windows 10;

7.7.6.9.5.iOS;

7.7.6.9.6. Android;

7.7.6.9.7. Mac OSX 10;

7.7.6.10. Deverá suportar os seguintes navegadores:

7.7.6.10.1. Internet Explorer 7 ou superior;

7.7.6.10.2. Firefox 3.6 ou superior;

7.7.6.10.3. Safari.

7.7.7. CONTROLE DE APLICAÇÕES WEB:

7.7.7.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB;

7.7.7.2. A solução deve ser capaz de identificar qualquer tipo de aplicação Web até camada 7, independente de porta e protocolo;

7.7.7.3. Possuir um reconhecimento de pelo menos 7100 aplicações diferentes, permitindo a consulta a base de aplicação em site público do fabricante, incluindo categorização para tráfego relacionado a aplicações peer-to-peer, redes sociais, acesso remoto, update de software, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

7.7.7.4. Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, social widgets com controle granular para usuários ou grupos de usuários;

7.7.7.5. A solução deverá prover controle de segurança granular de ao menos 250.000 Web 2.0 widgets

7.7.7.6. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund);

7.7.7.7. Deve possibilitar não apenas o bloqueio das aplicações, mas também de portas e protocolos. Deve ainda distinguir protocolos de aplicações, por exemplo o protocolo GRE não deve ser tratado como aplicação na política.

7.7.7.8. 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, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

7.7.7.9. 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. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta padrão ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 389;

7.7.7.10. Solução deve ser capaz de criar regras com várias categorias;

7.7.7.11. Deve possibilitar a permissão ou bloqueio de aplicações por pelos menos os seguintes critérios:

7.7.7.11.1. Aplicação da Web;

7.7.7.11.2. Categorias;

7.7.7.11.3. Nível de risco;

7.7.7.11.4. IP/Range de IP's/Redes;

7.7.7.11.5. Usuários do AD/LDAP;

7.7.7.12. Diferentes grupos de usuários;

7.7.7.13. Aplicações que sejam passiveis a técnicas de evasão por malwares e uso excessivo de banda como (ultrasurf, torrent, dropbox e file sharing);

7.7.7.14. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

7.7.7.15. Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e gerência;

7.7.7.16. 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;

7.7.7.17. Deve suportar o controle de aplicações conhecidas e possibilitar a inclusão de aplicações desconhecidas localmente, ou, através de ticket direto com o fabricante.

7.7.7.18. Deve possibilitar a customização, por regra, da tela de interação com o usuário, permitindo: informar, questionar e limitar a banda de acesso;

7.7.7.19. Deve permitir diferentes "telas" de interação com o usuário para dispositivos móveis;

7.7.7.20. Deve possibilitar a diferenciação e controle granular específico das aplicações: Gmail, Gmail Enterprise, Gmail-Drive, Gmail-file-transfer, Gmail-file-transfer-download, Gmail-file-transfer-upload, Inbox-by-Gmail, Gmail-chat, Gmail-video-chat, Gmail-Voice-Chat, Gmail-Voice-Video-Chat, Gmail-call-phone, Viber, Viber-file-transfer, Viber-Voice-Call, Viber-Voice-message, WhatsApp-Messenger, WhatsApp-Messenger-file-transfer, WhatsApp-Messenger-Web, WhatsApp-Messenger-Voice-Call;

7.7.7.21. Deve permitir o bloqueio de aplicações Proxies: Ultrasurf, GPass, FreeGate, Hopster, Tor, HotSpot Shield

7.7.7.22. Deve permitir o bloqueio de aplicações: AirVPN, ClickTools, G-Cloud-Backup, Hide.Me, Intacct, JumboMail, JumboMail-Download, JumboMail-Upload, JumboMail-Share, Nearby, PubNub, Sfax, Zapier, pCloud, skyZIP, AeroFS, Rocket-League, Tresorit, okta, Alexa, HubSpot, PingOne e VPN-Shield;

7.7.7.23. Deve possibilitar a integração da solução com base do Active Directory, Ldap, Radius ou base local para criação de políticas. Possibilitando a criação de regras utilizando:

7.7.7.23.1. Usuários;

7.7.7.23.2. Grupo de usuários;

7.7.7.23.3. Máquinas (estações de trabalho);

7.7.7.23.4. Endereço IP;

7.7.7.23.5. Endereço de Rede;

7.7.7.23.6. Combinação das opções acima;

7.7.7.24. Possuir controle granular para quais funcionalidades de proteção, endereços IPs será executada a inspeção e de-criptografia de SSL tanto para tráfego de entrada (Inbound) e Saída (Outbound).

7.7.7.25. A Solução deve ter um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem para um período de tempo específico;

7.7.7.26. Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);

7.7.7.27. Deve possibilitar a customização por regra utilizando as seguintes ações de controle:

7.7.7.27.1. Permitir;

7.7.7.27.2. Bloquear;

7.7.7.27.3. Monitorar;

7.7.7.27.4. Informar o usuário;

7.7.7.28. O mecanismo de Controle de aplicação deve apresentar contagem de utilização de regra de acordo com a utilização;

7.7.7.29. A solução deverá possuir uma interface de fácil utilização para buscas de Aplicações;

7.7.7.30. A solução deverá categorizar por Fator de Risco aplicações;

7.7.7.31. A solução deverá receber atualizações via internet para sua base;

7.7.7.32. A solução deverá possuir um mecanismo para informar ou perguntar ao usuário em tempo real com a finalidade de educá-los ou confirmar ações baseadas na política de acesso;

7.7.7.33. A solução deverá permitir a criação de exceções baseadas em objetos de rede;

7.7.7.34. A solução deve prover a opção de editar a notificação de bloqueio e redirecionar o usuário para a página de remediação;

7.7.7.35. A funcionalidade de Aplicação e filtros deverá possuir relatório de utilização.

7.7.8. IDENTIFICAÇÃO DE USUÁRIO:

7.7.8.1. Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP e Radius;

7.7.8.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

7.7.8.3. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

7.7.8.4. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

7.7.8.5. Deve possuir suporte a identificação de múltiplos usuários conectados com um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular;

7.7.8.6. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

7.7.8.7. Deve suportar autenticação para Smartphone e tablet's;

7.7.8.8. Deve suportar autenticação Kerberos transparente para single sign on;

7.7.8.9. A solução deverá compartilhar e propagar a identificação de usuários com outros gateways de segurança do mesmo fabricante;

7.7.8.10. Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;

7.7.8.11. A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

7.7.8.12. A solução de identificação de usuário deve suportar engine onde assume que um único usuário está conectado por computador;

7.7.8.13. A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

7.7.8.14. A solução deve integrar-se perfeitamente com serviços de diretório, IF-MAP e Radius;

7.7.8.15. A solução deve permitir a identificação de usuários através de proxy via "X-forward headers";

7.7.8.16. A solução deverá suportar grupos LDAP "nested";

7.7.9. CONTROLE DE URL:

7.7.9.1. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado ao Firewall NG;

7.7.9.2. A Solução deve ter um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem de URL para um período de tempo específico;

7.7.9.3. Deve possuir as seguintes funcionalidades de filtro de URL:

7.7.9.3.1. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

7.7.9.3.2. Deve ser possível a criação de políticas por Usuários e Grupos de Usuários cadastradas no AD, Ips, Redes e Grupos de Redes.

7.7.9.4. A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

7.7.9.5. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização;

7.7.9.6. Deverá ser possível questionar o usuário e obrigar o mesmo a justificar na própria página a necessidade do acesso, permitindo assim o registro em logs passíveis de auditoria;

7.7.9.7. A solução de Filtro de URL deverá ser totalmente integrada com a solução de Aplicações WEB 2.0 para melhor gerenciamento e controle Next Generation;

7.7.9.8. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund), sendo que para a opção de OUTBOUND não será necessário efetuar o MITM, ou seja, a solução deverá prover algum mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso de acordo com a política configurada;

7.7.9.9. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

7.7.9.10. A solução deve possuir engine de bloqueio de conteudo em sites de busca como (Google, Bing e Yahoo). Assim como o bloqueio de sites que estão em modo cashed;

7.7.9.11. Deve possibilitar a customização por regra com as seguintes ações de controle:

7.7.9.11.1. Permitir;

7.7.9.11.2. Bloquear;

7.7.9.11.3. Monitorar;

7.7.9.11.4. Informar o usuário;

7.7.9.12. Deverá 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 appliance (Captive Portal);

7.7.9.13. Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços.

7.7.9.14. Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs;

7.7.9.15. Deverá possuir pelo menos 60 categorias de URLs;

7.7.9.16. Deverá possibilitar a criação de Categorias de URLs customizadas;

7.7.9.17. Deverá possibilitar a exclusão de URLs do bloqueio por categoria;

7.7.9.18. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categoriza ou categorizada incorretamente;

7.7.9.19. Deve possibilitar a customização de pagina de bloqueio de interação com usuário;

7.7.9.20. Devem incluir informações das atividades dos usuários em seus logs;

7.7.9.21. Solução deve ter uma categorização URL que exceda 200 milhões de URLs;

7.7.9.22. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL.

7.7.10. PREVENÇÃO DE AMEAÇAS

7.7.10.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall sem a necessidade de uso de quaisquer interfaces externas onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança;

7.7.10.2.A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações;

7.7.10.3. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho sem degradar a performance do equipamento solicitado neste edital;

7.7.10.4. A solução de IPS deve fazer a inspeção de todo o trafego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;

7.7.10.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

7.7.10.6. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

7.7.10.7. Em cada proteção de segurança, deve estar incluso informações como: código CVE, tipo de impacto na ferramenta, severidade, e tipo de ação que a mesma irá executar;

7.7.10.8. A solução deve fazer captura de pacotes para proteções específicas;

7.7.10.9. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força a bruta a scanning de portas CIFS, Port overflow, Non Compliant SSL, IKE aggressive Exchange;

7.7.10.10. Deve ser capaz de bloquear tráfego SSH enviados em outras portas.

7.7.10.11. A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas;

7.7.10.12. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

7.7.10.13. As regras de exceção devem possuir: origem, destino e serviço;

7.7.10.14. A solução deve ser capaz de inspecionar tráfego HTTPS (inbound/Outbound);

7.7.10.15. Proteger o ambiente de ataque DoS;

7.7.10.16. Baseado nas melhores práticas de segurança e otimização de tempo operacional dos administradores, a solução de IPS integrada no appliance de segurança, deve possuir uma base de assinaturas de segurança superior a 5000 (cinco mil) assinaturas;

7.7.10.17. A solução de IPS deve possuir funcionalidade de simulação ou detecção do tráfego processado para fins de troubleshooting;

7.7.10.18. Na própria interface de gerência, a solução de IPS deve possuir índices por período (hora, semana ou mês) onde aponta o nível de ação das assinaturas baseada pela sua severidade;

7.7.10.19. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os appliances que estão sendo gerenciados informando no mínimo: Nome do Gateway, Endereços IP nas versões 4 e 6, Perfil Utilizado, Informação de status da funcionalidade de bypass e modo de operação (bloqueio ou detecção).

7.7.10.20. Para melhor administração da solução, a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

7.7.10.21. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção) das assinaturas recentemente baixadas via atualização sem alterar o padrão operacional do IPS previamente configurado;

7.7.10.22. . O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de mail, Web e DNS, onde as mesmas poderão ser assinaladas no momento da criação do objeto de rede na solução;

7.7.10.23. Deverá possibilitar a inclusão de novas assinaturas e customização no formato SNORT;

7.7.10.24. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

7.7.10.25. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

7.7.10.26. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, serviços Windows (Microsoft Networking) e VoIP;

7.7.10.27. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

7.7.10.28. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados

7.7.10.29. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

7.7.10.30. A solução deve permitir a pré-configuração de, no mínimo, 15 perfis de proteção de IPS que podem ser utilizados a qualquer momento;

7.7.10.31. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo das opções granulares em: última hora, últimas 24 horas, última semana e último mês;

7.7.10.32. A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens ou destinos e combinações entre os dois;

7.7.10.33. A solução deve permitir a configuração de políticas baseada em países, dispondo de pelo menos 220 países já cadastrados em sua base;

7.7.10.34. A solução deve possuir os seguintes esquemas de Update de assinaturas:

7.7.10.34.1. Update instantâneo, através de um click;

7.7.10.34.2. Update através de agendamento onde engloba horário, dias da semana ou dia do mês;

7.7.10.34.3. Update de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

7.7.10.35. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP de entrada. Depois de importar esses certificados, a solução deve permitir o uso desses certificados na configuração de regra de IPS para Inspeção segura HTTP;

7.7.10.36. Dentro a engine de inspeção HTTPS, a solução deve permitir a criação de diferentes regras onde será especificado: origem, destino, tipo de serviço, ação e certificado que será atribuído por regra;

7.7.10.37. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

7.7.10.38. A solução deverá permitir a criação de perfil de proteção baseado em hosts internos ou servidores ou a combinação dos dois;

7.7.10.39. A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato;

7.7.10.40. A solução deverá possuir proteções para sistemas SCADA;

7.7.10.41. A solução deverá inspecionar o protocolo Citrix com a finalidade de comprovar que o tráfego é realmente o protocolo Citrix ICA;

7.7.10.42. Solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados;

7.7.10.43. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

7.7.10.44. Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança ou entregue em composição com outro fabricante desde que integrado à gerência centralizada de administração, monitoração e logs;

7.7.10.45. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

7.7.10.46. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

7.7.10.47. Implementar funcionalidade de detecção e bloqueio de callbacks;

7.7.10.48. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

7.7.10.49. A solução Antibot deve possuir mecanismo de detecção em multi-camadas que inclui, reputação de endereço IP, URLs e endereços DNS e detectar padrões de comunicação, assinaturas e análise de mensagens de email;

7.7.10.50. Implementar atualização da base de dados da rede de inteligência de forma automática, permitindo o agendamento diários e período (tempo) de cada atualização;

7.7.10.51. Implementar mecanismo de múltiplas fases para verificação de malware e/ou códigos maliciosos;

7.7.10.52. A solução deve analisar e bloquear malware e/ou codigos maliciosos pelo menos nos seguintes tipos de arquivos: bat, com, exe, dll, vsd, reg, jar, txt, swf, cmd, mpg, jse, midi, mp3, hlp, php, png, TIF, WAV, ASF, HTM, COM, JPEG;

7.7.10.53. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, FTP e CIFS;

7.7.10.54. A solução deve atuar na prevenção de forma granular através de políticas por usuário / máquina ou Rede, sendo possível escolher um Profile diferente para cada regra;

7.7.10.55. A solução deve permitir criar regras de exceção de acordo com a proteção a partir do log visualizado na interface gráfica da gerência centralizada;

7.7.10.56. Implementar através da interface gráfica de administração, configuração de mecanismo de alerta onde seja possível configurar bloqueio/desbloqueio de uma comunicação do tipo callback;

7.7.10.57. A solução deve ser capaz de bloquear uma conexão até que a classificação da mesma seja completada.

7.7.10.58. Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados;

7.7.10.59. A solução deve possuir na própria interface de gerência, gráfico contento informações em tempo real sobre as atividades recentes de malwares detectados na solução, sendo que essas informações deverão ser apresentadas em mapa geográfico por país, através de IP ou URL e principais e-mails que foram scaneados;

7.7.10.60. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

7.7.10.61. A solução deve permitir de forma anônima compartilhar ou não informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do Fabricante;

7.7.10.62. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

7.7.10.63. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

7.7.10.64. Em caso de falha no mecanismo de inspeção do anti-virus, deve ser possível configurar se as conexões serão permitidas ou bloqueadas;

7.7.10.65. A solução de anti-bot e anti-virus, deve possuir recurso onde o administrador consiga criar as regras de politica de segurança, permitindo salva-las e posteriormente aplicar para entrar em modo detect/inspect.

7.7.10.66. Caso o administrador tenha realizado alteração na solução de anti-virus ou bot, essa funcionalidade deve possuir opção de aplicação de regra apenas nesta engine, sem interferir nas demais regras de outras funcionalidades de segurança. Assim evitando confronto com alteração de outras funcionalidades;

7.7.10.67. A solução deve ser capaz de procurar por ações de BOTs.

7.7.10.68. A solução deve suportar a detecção e prevenção de vírus Cryptors & ransmoware;

7.7.10.69. A solução deverá possuir mecanismo para proteger contra ataques de Spear phishing;

7.7.10.70. Analisar padrões de comunicação C&C e não apenas o servidor DNS destino;

7.7.10.71. Funcionalidade DNS TRAP, que visa auxiliar na descoberta de hosts infectados que geram comunicação com C&C;

7.7.10.72. Capacidade para detectar e prevenir ataque DNS tunneling;

7.7.10.73. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;

7.7.10.74. A solução deve ser capaz de prevenir acesso a websites maliciosos;

7.7.10.75. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

7.7.10.76. A solução deverá ser capaz de inspecionar arquivos comprimidos;

7.7.10.77. . A solução antivirus deverá suportar a análise de links no corpo de e-mails;

7.7.10.78. A solução antivirus deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS;

7.8. Lote 2 – Item 8 - Upgrade de licença de software de gerencia:

7.8.1. CARACTERÍSTICAS GERAIS:

7.8.1.1. O TRE-GO conta com licença válida da Check Point para 05 gateways administrados pelo sistema de gerência que deverá ser atualizada (upgrade) para comportar 10 gateways. A licença deverá ser de 5 anos.

7.8.1.2. Código da licença atual: CPSM-NGSM5;

7.8.1.3. Código da licença futura: CPSM-NGSM10;

7.8.1.4. Descrição da licença futura: Next Generation Security Management Software for 10 gateways (SmartEvent)

7.9. Lote 2 – Item 9 - Serviços de instalação e configuração dos equipamentos.

7.9.1. A CONTRATANTE disponibilizará espaço, refrigeração e infraestrutura elétrica com capacidade suficiente para comportar os equipamentos novos;

7.9.2. Todos os equipamentos fornecidos devem ser entregues instalados nos Datacenters do TRE-GO, conforme orientação da Coordenadoria de Infraestrutura da STI;

7.9.3. A CONTRATADA deverá:

7.9.3.1. Realizar a instalação física de todos os equipamentos fornecidos;

7.9.3.2. Atualizar os firmwares dos equipamentos fornecidos com as versões mais recentes até o momento da entrega;

7.9.3.3. Realizar a instalação de quaisquer softwares adicionais necessários à administração e operação dos equipamentos fornecidos;

7.9.3.4. Efetuar a transferência de conhecimento tecnológico, na modalidade hands-on, relativo a todos os itens fornecidos;

7.9.3.5. Fornecer todo ferramental necessário para execução dos serviços de instalação e configuração, incluindo softwares, equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias;

7.9.4. Os serviços que eventualmente acarretem risco aos sistemas em produção ou requeiram parada de servidores, equipamentos ou rede elétrica, somente poderão ser executados fora de expediente, podendo ser inclusive em finais de semana e feriados, em horários previamente acordados com a área de TI do TRE-GO;

7.9.5. Os serviços de instalação e configuração do equipamento, bem como a atividade de transferência de tecnologia, deverá ser executada pelo fabricante ou por profissional certificado pelo fabricante na solução fornecida;

7.9.6. Todo e qualquer custo envolvido na entrega, instalação, configuração e transferência de tecnologia deverá correr por conta da CONTRATADA, sem nenhum ônus para TRE-GO;

7.10. Item 10 - Switch gerenciável com 24 portas.

7.10.1. Requisitos de Interfaces:

7.10.1.1. CARACTERÍSTICAS GERAIS:

7.10.1.2. Equipamento tipo comutador gigabit ethernet com capacidade de operação em camada 2 do modelo OSI;

7.10.1.3. Deve ser fornecido com, 24 (vinte e quatro) portas 1000BASE-T Gigabit Ethernet, para conexão de cabos de par metálico UTP com conector RJ-45;

7.10.1.4. Deve ser fornecido com 2 slots para conexão de transceivers SFP para fibras ópticas multimodo com velocidade de 1GbE. Estas portas devem ser de uso simultâneo com as portas 1000Base-T e não serão aceitas interfaces do tipo combo;

7.10.1.5. Deve suportar Auto-MDIX e negociação automática de speed e duplex;

7.10.1.6. Deve possuir capacidade de vazão (taxa de encaminhamento) de pelo menos 26 (vinte e seis) Mpps;

7.10.1.7. Deve possuir tabela para, no mínimo, 8.000 (oito mil) endereços MAC;

7.10.1.8. Deve possuir Jumbo Frame de pelo menos 9000 bytes;

7.10.1.9. Possuir porta de console para ligação direta, de terminal RS-232 ou RJ-45 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

7.10.1.10. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, permitindo a criação de no mínimo 60 VLANs;

7.10.1.11. Deve possuir o protocolo “Network Time Protocol” (NTP) ou "Simple Network Time Protocol" SNTP, para a sincronização do relógio com outros dispositivos de rede;

7.10.1.12. Deve permitir configuração/administração remota através de SSH ou GUI Web HTTPS;

7.10.1.13. Deve permitir monitoramento via SNMP v1, v2 ou SNMPv3;

7.10.1.14. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136;

7.10.1.15. Gabinete padrão para montagem em rack de 19" ou half width rack (meia largura), com altura máxima de 1U, incluindo todos os acessórios para o perfeito funcionamento;

7.10.1.16. Deve ser equipamento de linha de produção atual do fabricante;

7.10.1.17. Deve possuir site do fabricante na Internet com descritivo de suas especificações técnicas;

8. ENTREGA, AVALIAÇÃO E ACEITE DOS SERVIÇOS

8.1. **Entrega:**

8.1.1. Os equipamentos e os softwares deverão ser entregues em até 30 (trinta) dias corridos após a emissão da Nota de Empenho;

8.1.2. Os equipamentos deverão ser entregues no TRE-GO - Praça Cívica, n° 300, Setor Central, Goiânia, Goiás, 5° andar, Ala B, na Seção de Suporte aos Serviços de Rede;

8.1.3. A Contratada deverá entregar os softwares e suas licenças por meio eletrônico pelo site do fabricante ou da Contratada, com opção de download ilimitado e acesso exclusivo ao Contratante ou, através de mídia física de instalação para a Seção de Suporte às Redes (SESRE);

8.1.4. A prestação dos serviços contratados deverá ser realizada após a emissão da Nota de Empenho e agendada com a Seção de Suporte às Redes (SESRE);

8.2. **Avaliação (Recebimento provisório):**

8.2.1. Será verificada a conformidade entre a especificação técnica dos equipamentos, softwares e serviços entregues com os itens descritos neste Termo de Referência num prazo máximo de 5 (cinco) dias úteis;

8.2.2. Caso seja constatada alguma desconformidade com o item 8.2.1, a Seção de Suporte às Redes (SESRE) comunicará a CONTRATADA para efetuar a correção dos problemas;

8.2.3. A correção estabelecida no item 8.2.2 deverá ser efetuada em até 10 (dez) dias úteis, contados a partir da data da comunicação;

8.3. **Termo de aceite (Recebimento definitivo):**

8.3.1. O termo de aceite técnico será emitido pela SESRE com ciência da Coordenadoria de Infraestrutura (CINF) em até 10 (dez) dias úteis após a entrega completa dos equipamentos e softwares, somente se estes atenderem plenamente todas as exigências deste Termo de Referência.

9. FORMA DE PAGAMENTO

9.1. A contratada deverá apresentar no ato da entrega dos produtos e serviços Nota Fiscal/Fatura para liquidação e pagamento da despesa pelo TRE-GO, após realizado o aceite pela equipe técnica da SESRE.

10. DEVERES E RESPONSABILIDADES DA CONTRATANTE

10.1. Efetuar o pagamento à Contratada, de acordo com as condições, no preço e no prazo estabelecidos;

10.2. Efetuar o recebimento definitivo em até 10 (dez) dias após o recebimento provisório dos produtos, exceto se houver atraso motivado pela Contratada;

10.3. Fornecer toda a infraestrutura necessária para a instalação dos produtos adquiridos;

11. DEVERES E RESPONSABILIDADES DA CONTRATADA

11.1. Fornecer os produtos e serviços no prazo e demais condições estipuladas.

11.2. Entregar os produtos instalados e configurados neste Regional, sem que isso implique acréscimo no preço constante da proposta.

11.3. Se constatada qualquer irregularidade nos produtos, a empresa deverá substituí-los, no prazo máximo de 10 (dez) dias úteis.

11.4. Não transferir a outrem, no todo ou em parte, o objeto contratado, sem prévia anuência do TRE-GO.

11.5. Manter durante a execução do contrato todas as condições de habilitação e qualificação exigidas na licitação.

11.6. Prestar suporte aos equipamentos e softwares, responsabilizando-se pela manutenção corretiva dos mesmos, durante o período de vigência do suporte/garantia, sem que isso implique acréscimo no preço constante da proposta.

11.7. Executar os serviços técnicos especializados utilizando profissional(is) capacitado(s) e certificado(s) pelo fabricante dos produtos e serviços descritos neste Termo de Referência;

12. QUALIFICAÇÃO TÉCNICA

12.1. Requisitos de Capacitação e Experiência:

12.1.1. Deverá possuir atestado de capacidade técnica emitido por instituição ou empresa de direito público ou privado no Brasil, comprovando que a licitante forneceu os produtos e os serviços de características semelhantes ao especificado neste termo de referência, prestando os devidos serviços de manutenção e suporte técnico;

12.1.2. No ato da proposta, o licitante deverá apresentar:

12.1.2.1. Catálogo oficial do fabricante, de acesso público através de website, onde poderão ser conferidas todas as características exigidas para o item e subitens que compõe o item ofertado, contento informações referentes à descrição e ao part number;

12.1.2.2. Declaração de que os equipamentos não estão descontinuados pelo fabricante.

13. GARANTIA E SUPORTE

13.1. Para os itens 1, 2 ,3, 4 e 7 deste Termo de Referência:

13.1.1. Deverão ter garantia de 60 (sessenta) meses on-site, incluindo suporte para Hardware e Software, prestado pelo fabricante dos equipamentos ou pela Contratada, com janela de abertura de chamado 24x7 e tempo de resposta de 24 horas, a partir do registro do chamado, e substituição do hardware em até 72 horas;

13.1.2. Serviço de atendimento 24x7 (incluindo finais de semana e feriados) através de linha telefônica 0800 do fabricante ou da Contratada (indicar na proposta) para abertura e gerenciamento de chamados técnicos e suporte de Software;

13.1.3. Entende-se como on-site o atendimento a ser realizado nas dependências do TRE-GO na cidade de Goiânia-GO;

13.2. Para o item 5:

13.2.1. Deverá ter suporte de 60 (sessenta) meses direto do fabricante;

13.2.2. Deverá fornecer o direito de “updates” e “upgrades” durante o período de suporte, sem custo adicional para o TRE-GO;

13.2.3. Serviço de atendimento 24x7 (incluindo finais de semana e feriados) através de linha telefônica 0800 do fabricante ou da Contratada (indicar na proposta) para abertura e gerenciamento de chamados técnicos e suporte do Software;

13.3. Para o item 10:

13.3.1. Deverá ter garantia de 36 (trinta e seis) meses on-site, incluindo suporte para Hardware e Software, prestado pelo fabricante dos equipamentos, com janela de abertura de chamado 8x5 e tempo de resposta de 24 horas, a partir do registro do chamado, e substituição do hardware em até 120 horas;

13.3.2. Serviço de atendimento 8x5 através de linha telefônica 0800 do fabricante ou da Contratada (indicar na proposta) para abertura e gerenciamento de chamados técnicos e suporte de Software;

13.3.3. Entende-se como on-site o atendimento a ser realizado nas dependências do TRE-GO na cidade de Goiânia-GO;

13.4. Regras de garantia e suporte que se aplicam a todos os equipamentos e softwares da solução:

13.4.1. Disponibilidade de website (indicar endereço) para suporte on-line, transferência de manuais e arquivos de configuração (device drives e firmware), e registro do equipamento e notificações automáticas de eventos do equipamento;

13.4.2. A CONTRATADA deverá fornecer garantia do fabricante dos equipamentos pelos períodos estabelecidos nos itens 13.1.1 e 13.3.1, contados a partir da emissão do Termo de Aceite Técnico (Recebimento Definitivo);

13.4.3. Deverão estar cobertos pela garantia todos os componentes físicos (hardware) e lógicos (software) que fazem parte deste Termo de Referência;

13.4.4. Deverão estar cobertas pela garantia quaisquer atualizações de firmware e software disponibilizadas pelo fabricante, bem como a realização dos procedimentos de instalação das atualizações;

13.4.5. Deverão estar cobertas pela garantia o fornecimento de partes e peças dos equipamentos, mão de obra, transporte, diárias, hospedagem e de quaisquer outros itens necessários à recuperação dos equipamentos ao estado de pleno funcionamento de todos os seus componentes;

13.4.5.1. Todas as partes de peças fornecidas deverão ser originais;

13.4.6. Todo e qualquer custo envolvido na prestação da garantia deverá correr por conta da CONTRATADA, sem nenhum ônus para o TRE-GO;

14. OBSERVAÇÕES TÉCNICAS GERAIS

14.1. Todos os itens fornecidos, incluído todos os seus componentes e acessórios, deverão ser novos e de primeiro uso;

14.1.1. Serão recusados os itens que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado novo pelo fornecedor dos itens;

14.2. Todos os itens devem ser fornecidos em pleno funcionamento, prontos para a utilização, com todos os acessórios e componentes;

ASSINATURA		
Integrante Técnico	**Integrante Demandante**	**Integrante Administrativo**
_____ ***Marcos Rogério Santiago*** ***SESRE***	_____ ***Marcílio Zaccarelli Bersaneti*** ***Coordenador de Infraestrutura***	_____ ***Priscila Oliveira Ataídes*** ***AGSAO/SAO***
Goiânia, 17 de Julho de 2019.		