TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Praça Desembargador Edgard Nogueira. S/Nº - Centro Civico - Bairro Cabral - CEP 64000920 - Teresina - PI - http://www.tre-pi.jus.br

PROCESSO : 0012283-09.2020.6.18.8000
INTERESSADO : SEÇÃO DE INFRAESTRUTURA
ASSUNTO :

Despacho nº 41988 / 2020 - TRE/PRESI/DG/STI/CODIN

Senhor Secretário,

Devolvo o presente com os documentos que integram os Estudos Preliminares referente à "*Aquisição de Solução de Firewall UTM/VPN*". São os documentos que compõem este processo:

1) a Análise de Viabilidade (1028711);

2) a Sustentação do Contrato (1037720);

3) a Análise de Riscos (1037766);

4) a Estratégia para a Contratação (1047596); e

5) o Termo de Referência (1048004), devendo ser desconsiderados os TRs (1039908 e 1047810).

Devido a complexidade da contratação foi necessário elaborar um documento anterior para consolidar o entendimento da solução antes de dar início a Análise de Viabilidade e outros documentos, esta consolidação está no documento Estudos Técnicos (1037463).

Para essa contratação foi priorizado um recurso orçamentário da monta de R$ 406.000,00 que previa a aquisição de dois equipamentos firewall da Sede e 82 equipamentos firewall para as Zonas Eleitorais.

Após a elaboração dos estudos verificamos que com a diminuição de postos de atendimentos a nossa necessidade foi alterada, entretanto também a previsão orçamentária ficou prejudicada pelo contexto atual de disparada do dólar, o que afeta diretamente os preços de equipamentos de tecnologia. Os estudos concluíram que a melhor solução para a aquisição é:

1) Contratação dos serviços de suporte e atualização para o *cluster* concentrador - Valor: R$ R$ 223.914,97;

2) Atualização da solução de firewall, com substituição dos equipamentos existentes, para os firewalls de pequeno porte - Valor: R$ R$ 396.940,48; e

3) Contratação de licença Global Management System (GMS) Sonicwall - Valor R$ R$ 196.597,39.

As licenças seriam para atualizar a nossa infraestrutura de solução firewall da Sonicwall e aquisição de licença para gerenciar toda a base instalada de equipamentos da Sonicwall. Esta solução totaliza R$ **817.452,84**, que está acima do orçamento priorizado.

Assim, a Equipe de Planejamento propõe que a aquisição seja realizada por registro de preços dos itens, conforme a tabela a seguir:

ITEM	DESCRIÇÃO	QUANTIDADE	DEMANDA	PREÇO

		REGISTRADA	INICIAL	UNITÁRIO MÁXIMO ACEITÁVEL
1	Contratação dos serviços de suporte, atualização e garantia para o *cluster* formado pelo Sonicwall NSA 5600, incluído a unidade de alta disponibilidade, com requisitos de segurança e serviços de suporte 24x7 cobertos pela **Garantia de 60 meses**. Referência: **01-SCC-1554**	1	1	R$ 223.914,97
2	Atualização da Solução de Firewall tipo pequeno porte com atualização dos equipamentos existentes para no mínimo o SonicWall SOHO 250 W, com serviço de suporte 8x5 cobertos pela **Garantia de 60 meses**. **Referências: 02-SCC-1865 / 02-SCC-1760**	68	24	R$ 5.837,36
3	Licença SonicWall Global Management System para até 70 nós por **36 meses**. Referências: a) 01 Licença **01-SSC-3311**; b) 02 Licenças **01-SSC-7664**; c) 01 Licença **01-SSC-3301**: d) 02 Licenças **01-SSC-6532**; e) 02 Licenças **01-SSC-6536**.	1	-	R$ 196.597,39

As demandas iniciais contemplam apenas os itens 1 e 2, e perfazem o montante de **R$ 364.011,61 (trezentos e sessenta e quatro mil e onze reais e sessenta e um centavos)**, portanto dentro do orçamento previsto.

A execução total registrada será avaliada durante a vigência da Ata de Registro de Preços, após considerar a economia obtida após a licitação das demais aquisições previstas para 2020 ou obtenção de recursos orçamentários que eventualmente possam surgir.

Informo que os documentos supracitados foram previamente avaliados em reunião do CGTI, o qual aprovou os Estudos e o Termo de Referência e solicitou que fosse acrescida mais uma proposta para o item 1 da solução, entretanto informo que na ocasião ainda não constava a Estratégia para a Contratação.

Ante o exposto, devolvo o presente para a análise e apreciação. Sendo aprovado, para envio à SAOF para a adoção dos procedimentos necessários à aquisição.

Atenciosamente,

ANTÔNIO MANOEL SILVEIRA DE SOUSA

Coordenador de Desenvolvimento e Infraestrutura

Documento assinado eletronicamente por **Antonio Manoel Silveira de Sousa**, **Coordenador de Desenvolvimento e Infraestrutura**, em 08/09/2020, às 09:58, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Alberto Ribeiro do Nascimento Junior**, **Técnico Judiciário**, em 16/10/2020, às 11:43, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1046244** e o código CRC **2497108B**.

PROPOSTA COMERCIAL

1. INFORMAÇÕES DA PROPOSTA

Nº documento:	INC_TREPI_07082020_001_RBS_PCOM	**Data:**	07/08/2020
Cliente:	Tribunal Regional Eleitoral do Piauí		
Objeto:	Firewall Médio Porte & Pequeno Porte / Licença para Firewall 5600 / E-security / GMS / SMA / Capture Client - antivírus		
Fabricante:	Sonicwall		
Contato:	Carlos Alberto R. do Nascimento Jr		

2. INFORMAÇÕES COMPLEMENTARES

Validade da Proposta:	45 dias corridos a partir da data de emissão.
Valores:	Valores expressos em Reais, com impostos inclusos.
Prazo de Entrega:	30 dias úteis.
Prazo de Pagamento:	15 dias após a entrega.

3. DADOS DA EMPRESA

Razão Social:	NOVA SERVICOS DE TECNOLOGIA DA INFORMACAO E NETWORKING EIRELLI
CNPJ:	10.685.932/0001-79
I.E.:	07.517.723/001-26
Endereço:	ST SRTV/SUL QUADRA 701 BLOCO O Nº 110 SALA 889A - ED. MULTIEMPRESARIAL – ASA SUL – CEP 70.340-000 - BRASILIA/DF

4. DADOS BANCÁRIOS

Banco:	Banco Sicoob (756)
Agência/Praça:	4001 – Brasília – DF
Conta Corrente:	115241-6

5. VALORES

Essa proposta contempla a aquisição de:

- solução de Firewall de médio porte + HA e licenciamento (5650 + AGSS);
- licenciamento para NSa 5600 em dois modelos: AGSS ou CGSS;
- firewall de pequeno porte SOHO 250-W com suporte 8x5 em dois modelos: 3 anos ou 5 anos;
- Firewall de pequeno porte SOHO-W com suporte 8x5 de 3 anos;
- solução de antis-spam (E-mail Security);
- Solução de gerenciamento centralizado (GMS), solução de acesso seguro – VPN (SMA);
- NGAV – antívirus de nova geração (Capture Client).

5.1. NSA 5650

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
NSA 5650 + HA + AGSS 5YR					
01	01	**01-SSC-1939** - SONICWALL NSA 5650 APPLIANCE	01	R$ 95.257,69	R$ 95.257,69
	02	**01-SSC-3217** - SONICWALL NSA 5650 HIGH AVAILABILITY	01	R$ 66.710,71	R$ 66.710,71
	03	**01-SSC-3678** - ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 5650 5YR	01	R$ 175.886,45	R$ 175.886,45
VALOR TOTAL DA PROPOSTA:		**R$ 337.854,85 (Trezentos e trinta e sete mil, oitocentos e cinquenta e quatro reais e oitenta e cinco centavos)**			

5.2. AGSS – NSA 5600

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
AGSS NSA 5600 POR 5 ANOS					
02	01	**01-SSC-1554** - ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 5600 5YR	01	R$ 223.914,97	R$ 223.914,97
VALOR TOTAL DA PROPOSTA:		**R$ 223.914,97 (Duzentos e vinte e três mil, novecentos e quatorze reais e noventa e sete centavos)**			

5.3. CGSS – NSA 5600

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
CGSS NSA 5600					
03	01	**01-SSC-4238** - COMPREHENSIVE GATEWAY SECURITY SUITE FOR NSA 5600 (5 YR)	01	R$ 173.340,76	R$ 173.340,76
VALOR TOTAL DA PROPOSTA:		**R$ 173.340,76 (Cento e setenta e três mil, trezentos e quarenta reais e setenta e seis centavos)**			

5.4. SOHO 250W + SUPORTE 8X5 – 3 ANOS

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
SOHO 250W + SUPORTE 8X5 – 5 ANOS					
05	01	**02-SSC-1865** - SONICWALL SOHO 250 WIRELESS-N INTL	68	R$ 4.869,30	R$ 331.112,40
	02	**02-SSC-1758** - STANDARD SUPPORT FOR SOHO 250 SERIES 3YR	68	R$ 1.493,16	R$ 101.534,88
VALOR TOTAL DA PROPOSTA:		**R$ 432.647,28 (Quatrocentos e trinta e dois mil, seiscentos e quarenta e sete reais e vinte e oito centavos)**			

5.5. SOHO 250W + SUPORTE 8X5 – 5 ANOS

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
SOHO 250W + SUPORTE 8X5 – 3 ANOS					
04	01	**02-SSC-1865** - SONICWALL SOHO 250 WIRELESS-N INTL	68	R$ 4.869,30	R$ 331.112,40
	02	**02-SSC-1760** - STANDARD SUPPORT FOR SOHO 250 SERIES 5YR	68	R$ 2.455,42	R$ 166.968,56
VALOR TOTAL DA PROPOSTA:		**R$ 498.080,96 (Quatrocentos e noventa e oito mil, oitenta reais e noventa e seis centavos)**			

5.6. SOHO W + SUPORTE 8X5 – 3 ANOS

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
SOHO W + SUPORTE 8X5 – 3 ANOS					
06	01	**01-SSC-0644** - SONICWALL SOHO WIRELESS-N INTL	68	R$ 4.747,35	R$ 322.819,80
	02	**01-SSC-0696** - STANDARD SUPPORT FOR SOHO SERIES 3YR	68	R$ 1.454,95	R$ 98.936,60
VALOR TOTAL DA PROPOSTA:		**R$ 421.756,40 (Quatrocentos e vinte e um mil, setecentos e cinquenta e seis reais e quarenta centavos)**			

5.7. EMAIL SECURITY

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
07	01	**01-SSC-7636** - SONICWALL EMAIL VIRTUAL APPLIANCE - 1 SERVER LICENSE	01	R$ 4.603,85	R$ 4.603,85
	02	**01-SSC-7418** - SONICWALL TOTALSECURE EMAIL SUBSCRIPTION 1,000 (3 YRS)	01	R$ 124.652,24	R$ 124.652,24
	03	**01-SSC-7426** - SONICWALL TOTALSECURE EMAIL SUBSCRIPTION 100 (3 YEARS)	01	R$ 26.555,34	R$ 26.555,34
	04	**01-SSC-1534** - CAPTURE FOR SNWL TOTALSECURE EMAIL SUBSCRIPTION 1,000U 3YR	01	R$ 24.930,45	R$ 24.930,45
	05	**01-SSC-1876** - CAPTURE FOR SNWL TOTALSECURE EMAIL SUBSCRIPTION 100U 3YR	01	R$ 5.307,97	R$ 5.307,97
	06	**01-SSC-8531** - SONICWALL REMOTE IMPLEMENTATION EMAIL SECURITY	01	R$ 11.567,67	R$ 11.567,67
VALOR TOTAL DA PROPOSTA:		**R$ 197.617,52 (Cento e noventa e sete mil, seiscentos e dezessete reais e cinquenta e dois centavos)**			

5.8. GMS

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
08	01	**01-SSC-3311** - SONICWALL GMS 25 NODE SOFTWARE LICENSE	01	R$ 46.309,35	R$ 46.309,35
	02	**01-SSC-7664** - SONICWALL GMS 10 NODE SOFTWARE UPGRADE	02	R$ 18.957,05	R$ 37.914,10
	03	**01-SSC-3301** - SONICWALL GMS 25 NODE SOFTWARE UPGRADE	01	R$ 41.666,81	R$ 41.666,81
	04	**01-SSC-6532** - SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 10 NODES (3 YEARS)	02	R$ 7.598,29	R$ 15.196,58
	05	**01-SSC-6536** - SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 25 NODES (3 YEARS)	02	R$ 19.026,68	R$ 38.053,36
VALOR TOTAL DA PROPOSTA:		**R$ 179.140,20 (Cento e setenta e novo mil, cento e quarenta reais e vinte centavos)**			

5.9. SMA

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
09	01	**01-SSC-8468** - SMA 8200V VIRTUAL APPLIANCE	01	R$ 15.436,45	R$ 15.436,45
	02	**01-SSC-2054** - SMA POOLED PERPETUAL FULL LICENSE 50 USER	01	R$ 30.950,28	R$ 30.950,28
	03	**01-SSC-2077** - SMA POOLED PERPETUAL 24X7 SUPPORT 50 USER 3 YEARS	01	R$ 27.081,49	R$ 27.081,49
	04	**01-SSC-4357** - SONICWALL REMOTE IMPLEMENTATION SMA 1000 SERIES	01	R$ 15.475,14	R$ 15.475,14
VALOR TOTAL DA PROPOSTA:		**R$ 88.943,36 (Oitenta e oito mil, novecentos e quarenta e três reais e trinta e seis centavos)**			

5.10. CAPTURE CLIENT

GRUPO	ITEM	ESPECIFICAÇÃO – DESCRIÇÃO DOS PRODUTOS	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
10	01	**02-SSC-1458** - SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS 3YR	1.100	R$ 727,33	R$ 800.063,00
VALOR TOTAL DA PROPOSTA:			**R$ 800.063,00 (Oitocentos mil e sessenta e três reais)**		

Jacob Nácul

Diretor Executivo

jacob@inovazul.com.br

(61) 3703-4444

NTSEC
NETWORK SECURITY

PROPOSTA COMERCIAL

Matriz (Brasília)
Tel.: +55 (61) 3248-3829
contato@ntsec.com.br

São Paulo, 28 de agosto de 2020.

Ao Tribunal Regional Eleitoral do Piauí
A/C: Sr.: Carlos Alberto Ribeiro do Nascimento Jr
PROPOSTA Nº 128/20 V1.0

Prezados,

É com grande satisfação que encaminhamos proposta comercial estimativa para aquisição de produtos e serviços do fabricante Check Point.

Agradecemos a oportunidade e a confiança depositada na **NTSec | Network Security** e esperamos poder estreitar ainda mais o nosso relacionamento.

Em caso de dúvida ou questionamento, entre em contato conosco. Estamos à disposição para atendê-lo.

Atenciosamente,

Peterson Muzeli
NTSec | Network Security
Celular: (11) 99218-4783
Telefone: (61) 3248-3829

NTSEC
NETWORK SECURITY

Sumário

1. Carta de Apresentação

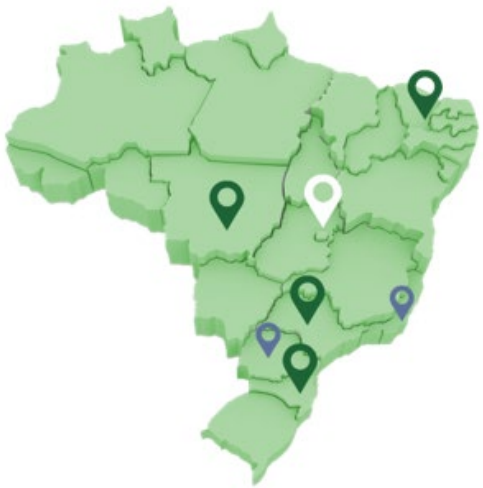
A **NTSec** é uma empresa focada em prover serviços técnicos especializados e integrar soluções em tecnologia da informação, reconhecida por proteger com eficácia negócios empresariais há mais de 10 anos.

Possuímos NOC (Network Operation Center) e uma equipe técnica especializada, permitindo o monitoramento e gestão dos eventos de TI, atuando de forma preventiva e proativa com o objetivo de manter o ambiente dos nossos clientes o mais estável possível.

2. Termo de Confidencialidade

Todas as informações, contidas ou reveladas neste documento, a partir daqui referenciadas apenas como 'Informações confidenciais', são de propriedade da NTSec | Network Security. Estas informações confidenciais são compartilhadas para fins de avaliação da Proposta Comercial para o projeto em questão. A aceitação deste material implica que essas informações confidenciais serão usadas somente com esta finalidade, e que as mesmas serão mantidas em sigilo, não serão reproduzidas, reveladas a terceiros ou usadas, totalmente ou parcialmente, sem permissão expressa e por escrito da NTSec | Network Security

3. Onde estamos



Matriz:
- Brasília – DF

Filiais:
- São Paulo - SP
- Cuiabá - MT
- Fortaleza - CE
- Florianópolis - SC

Presença:
- Rio de Janeiro - RJ
- Curitiba - PR

NTSEC
NETWORK SECURITY

4. Nossos parceiros

Check Point · Symantec · vmware · CYBERARK · IBM Security · ixia · PICUS SECURITY · PURESTORAGE

CLOUDFLARE · BACKBOX · aruba a Hewlett Packard Enterprise company · A10 · NUTANIX · VEEAM · Lenovo · SOPHOS

5. Algumas de nossas certificações

Nutanix Certified Professional (NCP)

Cisco CCNA Routing and Switching

Cisco CCNA Routing and Switching

GIAC Certified Incident Handler (GCIH)

VMware Certified Professional – Network Virtualization

VMware Certified Professional – Data Center Virtualization

6. Principais clientes

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO E SERVIÇOS · MPT · MINISTÉRIO DO DESENVOLVIMENTO SOCIAL E AGRÁRIO · MINISTÉRIO DA INTEGRAÇÃO NACIONAL · SUDAM

ICTS · NCHIETA · ANAC · BANCO DO BRASIL · TRT2 · TST

BRB BANCO DE BRASÍLIA · DETRAN DF · TRTsc · SESCOOP · Sesc DISTRITO FEDERAL

BANCO CENTRAL DO BRASIL · CABAL · caesb · CELG · CITEX

7. Centro de treinamento e certificação

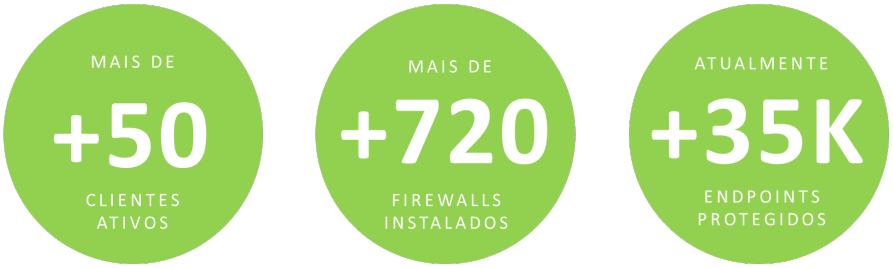
Oferecer soluções de segurança para nossos clientes é ótimo, mas transformá-los em melhores profissionais é incrível! A NTSEC leva isso a sério e está empenhada em garantir que os nossos clientes dominem as soluções que possuem, otimizando a utilização dos recursos e gerando os resultados esperados.

CHECK POINT STARS PARTNER – AUTHORIZED TRAINING CENTER

aruba a Hewlett Packard Enterprise company – AUTHORIZED TRAINING CENTER

PEARSON VUE – AUTHORIZED TEST CENTER

8. Alguns de nossos números



9. Proposta comercial

9.1. Objeto da proposta

Aquisição de produtos e serviços do fabricante Check Point.

9.2. Investimento

SKU	Quantity	Name	Valor Unitário R$	Valor Total R$
CPAP-SG1590	68	1590 Next Generation Appliance	R$ 11.044,60	R$ 751.032,80
CPSB-NGFW-CO-PREM-1590-5Y	68	Next Generation Firewall (NGFW) Package subscription & Collaborative Premium support for 1590 Appliance, for 5 Years	R$ 20.985,20	R$ 1.426.993,60
CPAP-SG6700-PLUS-SNBT	2	6700 Plus appliance with SandBlast subscription package for 1 year	R$ 285.729,00	R$ 571.458,00
CPSB-SNBT-6700-PLUS-3Y	2	Next Generation Threat Prevention and Sandblast for additional 3 years for 6700 PLUS Appliance	R$ 341.433,85	R$ 682.867,70
CPSB-SNBT-6700-PLUS-1Y	2	Next Generation Threat Prevention and Sandblast for additional 1 year for 6700 PLUS Appliance	R$ 113.810,90	R$ 227.621,80
CPAP-NGSM5150-MLOG10	1	Smart-1 5150 appliance Multi-Log Manager for 150 gateways and 10 domains (perpetual)	R$ 432.194,15	R$ 432.194,15
CPSB-EVS-COMP-150-3Y	1	SmartEvent, SmartReporter and Compliance blades for 150 gateways (Smart-1 & open server) 3 year subscription	R$ 626.682,15	R$ 626.682,15
CPSB-EVS-COMP-150-1Y	1	SmartEvent, SmartReporter and Compliance blades for 150 gateways (Smart-1 & open server) 1 year subscription	R$ 208.894,05	R$ 208.894,05
Valor Total da Proposta				**R$ 4.927.744,25**

Valor total da proposta: R$ 4.927.744,25 (Quatro milhões, novecentos e vinte e sete mil, setecentos e quarenta e quatro reais e vinte e cinco centavos).

9.3. Validade

A proposta estimativa em questão tem validade de 7 (sete) dias corridos a contar da sua emissão. Decorrido este prazo, a NTSEC – NETWORK SECURITY® reserva-se o direito de alterar, corrigir e/ou reajustar valores, bem como todas as demais condições técnicas e/ou comerciais apresentadas nesta proposta comercial.

9.4. Forma de Pagamento

Com preços expressos em reais (R$), com pagamento em 30 (trinta) dias corridos após o faturamento.

9.5. Prazo de entrega

Os produtos ofertados serão entregues em até 30 (trinta) dias, contados após o processamento do pedido.

10. Dados da empresa

Dados Empresa:
Razão Social: NTSec Soluções em Teleinformática LTDA
CNPJ: 09.137.728/0001-34
Endereço: SCN QD 05 Torre Norte Sala 617
Ed. Brasília Shopping - Asa Norte
Brasília – DF – CEP: 70715.900

11. Dados Bancários

Banco do Brasil 001
Agência: 0452-9
Conta Corrente: 500700-3

São Paulo, 28 de agosto de 2020.

Peterson Muzeli
Diretor Regional Sudeste
CPF: 213.313.488-38

TRE
PARANÁ

Publicado em: 23/01/2020
Vigência: 39 meses
Início: 08/01/2020
Término: 07/04/2023

CONTRATO Nº 04/2020

PAD nº 16459/2019

CONTRATO DE FORNECIMENTO E GARANTIA que entre si fazem o TRIBUNAL REGIONAL ELEITORAL DO PARANÁ e a empresa NTSEC SOLUCOES EM TELEINFORMATICA LTDA (NETWORK SECURITY)

Pelo presente instrumento, regido pela Lei nº 8.666 de 21.06.93, regida pela Lei nº 10.520/02, Lei Complementar nº 123/06, Lei nº 11.488/2007, pelos Decretos n.º 10.024/2019 e nº 8.538/2015, e em conformidade com o Termo de Abertura de Licitação nº 38/2019, Pregão Eletrônico nº. 66/2019 - Registro de Preços, e a proposta vencedora, protocolada neste Tribunal sob o PAD principal nº. 6279/2019, regularmente autorizada pelo ordenador de despesas;

O **TRIBUNAL REGIONAL ELEITORAL DO PARANÁ,** inscrito no **CNPJ sob nº. 03.985.113/0001-81,** com sede na Rua João Parolin, nº. 224, Prado Velho, Curitiba/PR, CEP: 80.220-902, telefone: (41) 3330-8500, neste ato representado por sua Diretor-Geral, Dr. Valcir Mombach, doravante denominado CONTRATANTE, e a empresa:

NTSEC SOLUCOES EM TELEINFORMATICA LTDA (NETWORK SECURITY), inscrita no **CNPJ sob nº 09.137.728/0001-34,** com sede em Brasília/DF, SCN, Quadra 05, bloco A, nº 50, sala 617, Ed. Brasília Shopping, Asa Norte, CEP: 70715-900, telefone: (61) 3248-3829, (61) 3037-7907 e (61) 8173-7982, e-mail: licitacao@ntsec.com.br, contato@ntsec.com.br, neste ato representada por Patricia Angelina da Conceição, portadora do CPF/MF nº. 346.994.838-01, doravante denominada CONTRATADA; têm entre si justo e acertado o que segue:

CLÁUSULA PRIMEIRA: DO OBJETO

1.1 – A presente contratação tem por objeto o **fornecimento e garantia** de solução de proteção de rede com características de ***Next Generation Firewall (NGFW)*** para segurança de informação perimetral que inclui filtro de pacotes, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, *spywares e malwares "Zero Day"*, Filtro de URL, funcionalidade de *Sandbox,* bem como controle de transmissão de dados e acesso à Internet compondo uma plataforma de segurança[1] integrada com garantia e respectiva subscrição por, pelo menos, 36 (trinta e seis) meses, ITEM 1, conforme especificações descritas neste Contrato.

[1] Por plataforma de segurança entende-se hardware e software integrados do tipo *appliance*

1.2 - A Contratação obedecerá ao estipulado neste contrato, bem como às disposições do instrumento convocatório, que, independentemente de transcrição, fazem parte integrante e complementar deste.

CLÁUSULA SEGUNDA: DAS ESPECIFICAÇÕES TÉCNICAS

2.1 – Aquisição dos itens abaixo informados:

	Item	Descrição	Quantidade
LOTE 1	1	*Appliance Next Generation Firewall (NGFW)*, com interface de gerência e respectivas licenças, garantia, suporte e atualizações por 36 meses	02

2.2 - Descrição do item e requisitos técnicos mínimos:

2.2.1 – ITEM 1 - *Appliance Firewall* NGFW:

2.2.1.1 - Entende-se por "*Appliance Firewall* NGFW", conjunto formado por *hardware* e respectivas licenças de *software* necessárias para seu funcionamento, incluídas as consoles de gerência e monitoramento.

2.2.1.1.1 - Para atendimento a esse item será aceito o fornecimento do *hardware* em *appliance* composto por 02 (dois) equipamentos, desde que atendidas todas as características, as funcionalidades e as capacidades descritas neste termo de referência.

2.2.1.2 - Cada *"Appliance* NGFW" deve possuir as seguintes características, licenciadas para uso:

2.2.1.2.1 - Possuir *throughput* mínimo de 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: Firewall, Controle de aplicação, IPS, Antivírus e *Anti-spyware*. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado.

2.2.1.2.2 - Os *throughputs* devem ser comprovados por documento de domínio público do fabricante. A localização destes documentos deve ser informada na proposta detalhada (conforme item 8.3 do edital). A ausência/inexistência de tais documentos resultará desclassificação da proposta.

2.2.1.2.3 - Os documentos públicos devem comprovar os *throughputs* aferidos com tráfego HTTP ou **blend** de protocolos definidos pelo fabricante como tráfego real (*real-world traffic blend*).

2.2.1.2.4 - Não será aceita aceleração de pacotes na placa de rede limitando a análise somente até camada 4.

2.2.1.2.5 - Deve ser capaz de suportar, no mínimo, 1.000.000 conexões simultâneas.

2.2.1.2.6 - Deve ser capaz de suportar, no mínimo, 55.000 novas conexões por segundo.

2.2.1.2.7 - Deve ser fornecido com fontes 120/240 AC, redundantes, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

2.2.1.2.8 - Deve ser fornecido com *coolers* ou *fans hot-swappables*, ou seja, estes elementos devem permitir a sua substituição sem que seja necessário desligar o equipamento.

2.2.1.2.9 - Deve ser fornecido com disco *Solid State Drive* (SSD) com no mínimo 2400 GB.

2.2.1.2.10 - Deve possuir, no mínimo, 08 (oito) interfaces de rede 10/100/1000 base-TX.

2.2.1.2.11 - Deve possuir, no mínimo, 04 (quatro) interfaces de rede 10 Gbps SFP+, fornecidos com seus respectivos *transceivers* do tipo SR.

2.2.1.2.12 - Deve possuir 01 (uma) interface de rede 1 Gbps dedicada para gerenciamento.

2.2.1.2.13 - Deve possuir 01 (uma) interface do tipo console ou similar.

2.2.1.2.14 - Deve ser capaz de operar em alta disponibilidade nos modos Ativo/Ativo ou Ativo/Passivo.

2.2.1.2.15 - Os equipamentos (*appliances*) fornecidos (Alta disponibilidade) devem possuir o mesmo fabricante, modelo e configuração.

2.2.1.2.16 - Deve suportar, no mínimo, 50 (cinquenta) zonas de segurança.

2.2.1.2.17 - Deve permitir a expansão futura de, no mínimo, 04 (quatro) instâncias virtuais de *firewall*.

2.2.1.2.18 - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 300 (trezentos) clientes de VPN SSL simultâneos.

2.2.1.2.19 - Deve ser fornecido com licenciamento ou suporte sem a necessidade de licença adicional para, no mínimo, 50 (cinquenta) túneis de VPN IPSEC simultâneos.

2.2.1.3 - Por cada equipamento que compõe a plataforma de segurança, entende-se o *hardware* e as licenças de *softwares* necessárias para o seu funcionamento.

2.2.1.4 - Por console de gerência e monitoração, entende-se as licenças de *software* necessárias para as duas funcionalidades.

2.2.1.5 - A console de gerência e monitoramento não pode residir no mesmo *appliance* de proteção de rede, devendo ser segregadas dos equipamentos dos *appliances* de proteção.

2.2.1.5.1 - A console de gerência e monitoramento deve ser virtual e deve rodar em ambiente VMWare ESXi 6.0 ou superior.

2.2.1.6 - Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em como *end-of-life* ou *end-of-sale*.

2.2.1.7 - Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", e devem incluir kit tipo trilho para adaptação, se necessário, e cabos de alimentação.

2.2.1.8 - A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência e monitoração.

2.2.1.9 - Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

2.2.1.10 - As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

2.2.1.11 - A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

2.2.1.12 - O *hardware* e *software* que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

2.2.1.13 - O *software* deverá ser fornecido em sua versão mais atualizada recomendada pelo fabricante.

2.2.1.14 - Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

a) Suporte a 1024 VLAN Tags 802.1q
b) Agregação de links 802.3ad e LACP
c) Policy based routing ou policy based forwarding
d) Roteamento multicast (PIM-SM)
e) DHCP Relay
f) DHCP Server
g) Suporte à criação de objetos de rede

2.2.1.15 - Suportar sub-interfaces ethernet logicas.

2.2.1.15.1 - Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de *firewall* ou roteamento baseado em políticas (PBR).

2.2.1.16 - O *firewall* deve ter a capacidade de testar o funcionamento de rotas estáticas ou rota *default* com a definição de um endereço IP de destino que deve estar comunicável por meio de uma rota. Caso haja falha na comunicação o *firewall* deve ter a capacidade de usar rota alternativa para estabelecer a comunicação.

2.2.1.17 - Deve suportar os seguintes tipos de NAT:

a) Nat dinâmico (*Many-to-1*);
b) Nat dinâmico (*Many-to-Many*);
c) Nat estático (1-to-1);
d) NAT estático (*Many-to-Many*);
e) Nat estático bidirecional 1-to-1;
f) Tradução de porta (PAT);
g) NAT de Origem;
h) NAT de Destino;
i) Suportar NAT de Origem e NAT de Destino simultaneamente.

2.2.1.18 - Deve implementar o protocolo ECMP.

2.2.1.19 - Deve implementar balanceamento de link por pelo menos um dos métodos a seguir: IP de origem, IP de origem e destino ou *round-robin*.

2.2.1.20 - Enviar log para sistemas de monitoração externos, simultaneamente.

2.2.1.21 - Deve haver a opção de enviar logs para os sistemas de monitoração externos.

2.2.1.22 - Proteção de *anti-spoofing*;

2.2.1.23 - Dever permitir bloquear conexões que contenham dados no *payload* de pacotes durante o *three-way hand-shake*;

2.2.1.24 - Deve exibir nos logs de tráfego o motivo para o término da sessão no *firewall*, incluindo sessões finalizadas onde houver de-criptografia de SSL ou SSH.

2.2.1.25 - Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

2.2.1.26 - Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

2.2.1.27 - Suportar a OSPF *graceful restart*;

2.2.1.28 - Deve suportar o protocolo BGP permitindo que o *firewall* possa anunciar rotas para IPv6.

2.2.1.28.1 - Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (*address auto configuration*), NAT64, Identificação de usuários a partir do LDAP/AD, *Captive* Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (*Denial of Service*), De-criptografia SSL ou SSH, PBF (*Policy Based Forwarding*), DHCPv6 *Relay*, IPSec, VPN SSL, Ativo/Passivo, SNMP, NTP, DNS e controle de aplicação.

2.2.1.29 - Os dispositivos de proteção devem ter a capacidade de operar mediante o uso de suas interfaces físicas nos seguintes modos: Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3).

2.2.1.29.1 - Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

2.2.1.29.2 - Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

2.2.1.29.3 - Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas.

2.2.1.30 - Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:

a) Em modo transparente;
b) Em layer 3.

2.2.1.31 - A configuração em alta disponibilidade deve sincronizar:

a) Sessões;
b) Configurações, incluindo, mas não limitado a políticas de *Firewall*, NAT, QOS e objetos de rede;

c) Associações de Segurança das VPNs;
d) Tabelas FIB.

2.2.1.32 - O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

2.2.1.33 - As funcionalidades de filtro de pacotes, NAT, VPN IPSec e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *software* com o fabricante.

2.2.1.34 - Controle por política de *Firewall*

2.2.1.34.1 - Deverá suportar controles por zona de segurança.

2.2.1.34.2 - Controles de políticas por porta e protocolo.

2.2.1.34.3 - Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras.

2.2.1.34.4 - A solução deve identificar de forma automática quais interfaces o tráfego irá ser direcionado, evitando assim que as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.

2.2.1.34.5 - Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

2.2.1.34.6 - Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

2.2.1.34.7 - Deve permitir consultar ou criar políticas para objetos das listas externas ou nuvem de inteligência do fabricante a partir da interface de gerência do próprio firewall.

2.2.1.34.8 - Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

2.2.1.34.9 - Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada *(Inbound)* e Saída (*Outbound*).

2.2.1.34.10 - Deve de-criptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1.2.

2.2.1.34.11 - Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo *Elliptical Curve Digital Signature Algorithm (ECDSA);*

2.2.1.34.12 - Controle de inspeção e de-criptografia de SSH ou SSL por política.

2.2.1.34.13 - Bloqueio de, no mínimo, os seguintes tipos de arquivos: cab, msi e exe.

2.2.1.34.14 - *Traffic shaping* QoS baseado em Políticas (Prioridade, Garantia e Máximo).

2.2.1.34.15 - Suporte a objetos e regras IPV6.

2.2.1.34.16 - Suporte a objetos e regras *multicast.*

2.2.1.34.17 - Deve suportar no mínimo dois dos tipos de negação de tráfego nas políticas de *firewall* a seguir: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP *Unreachable* para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão.

2.2.1.34.18 - Suportar a atribuição de agendamento das políticas (ou regras) com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

2.2.1.35 - Controle de aplicações

2.2.1.35.1 - Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

2.2.1.35.2 - Deve ser possível efetuar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

2.2.1.35.3 - Deve reconhecer nativamente aplicações relacionadas a tráfego *peer-to-peer*, redes sociais, acesso remoto, *update* de *software*, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

2.2.1.35.4 - Deve reconhecer pelo menos as seguintes aplicações: *bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer*, rdp ou ms-rdp, vnc, gmail, *youtube*, *http-tunnel*, *facebook chat, gmail chat, whatsapp*, *4shared, dropbox, google drive, onedrive*, db2, mysql, *oracle, kerberos, ldap, radius, itunes,* dhcp, ftp, dns, *wins*, ntp, snmp, *gotomeeting, webex, evernote* e *google* ou *google-docs*;

2.2.1.35.5 - Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar por meio 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 *default* ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 3389;

2.2.1.35.6 - Deve detectar aplicações por meio de análise comportamental do tráfego observado, incluindo, pelo menos, *Encrypted Bittorrent* e aplicações VOIP.

2.2.1.35.7 - Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como *Skype* e ataques mediante a porta 443.

2.2.1.35.8 - Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

2.2.1.35.9 - Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a *Yahoo Instant Messenger* usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do *Webex*. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas.

2.2.1.35.10 - Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a *Skype*. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como *Skype* apenas para alguns usuários;

2.2.1.35.11 - Deve permitir controle granular para aplicações SaaS, tais como: *Office* 365, *Skype*, aplicativos *google, gmail*, etc.;

2.2.1.35.12 - Identificar o uso de táticas evasivas via comunicações criptografadas;

2.2.1.35.13 - Atualizar a base de assinaturas de aplicações automaticamente.

2.2.1.35.14 - Reconhecer aplicações em IPv6.

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

2.2.1.35.16 - Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente nas estações dos usuários.

2.2.1.35.17 - Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

2.2.1.35.18 - Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos: checagem de assinaturas e decodificação de protocolos.

2.2.1.35.19 - Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

2.2.1.35.20 - Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações da instituição.

2.2.1.35.20.1 - A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no *payload* dos pacotes TCP e UDP ou usando *decoders* de pelo menos os seguintes protocolos: HTTP, FTP, SMTP, Telnet, SSH, IMAP, IMAP e RTSP.

2.2.1.35.21 - O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

2.2.1.35.22 - Deve alertar o usuário quando uma aplicação for bloqueada.

2.2.1.35.23 - Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

2.2.1.35.24 - Deve possibilitar a diferenciação de tráfegos *Peer2Peer* (*Bittorrent, emule, neonet*, etc.) possuindo granularidade de controle/políticas para os mesmos.

2.2.1.35.25 - Deve possibilitar a diferenciação de tráfegos de *Instant Messaging* (AIM, *Gtalk, Facebook Chat*, etc.) possuindo granularidade de controle/políticas para os mesmos.

2.2.1.35.26 - Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o *Gtalk* chat e bloquear a transferência de arquivos.

2.2.1.35.27 - Deve possibilitar a diferenciação de aplicações *Proxies* (*ghostsurf, freegate*, etc.) possuindo granularidade de controle/políticas para os mesmos.

2.2.1.35.28 - Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

a) Tecnologia utilizada nas aplicações (*Client-Server, Browser Based, Network Protocol*, etc.);
b) Nível de risco da aplicação;
c) Categoria e subcategoria de aplicações;
d) Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda, etc.

2.2.1.36 - Prevenção de ameaças

2.2.1.36.1 - Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e *Anti-Spyware* (ou *antimalware*) integrados no próprio *appliance* de *Firewall* ou entregue por meio de composição com outro equipamento ou fabricante.

2.2.1.36.2 - Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware* ou *antimalware*).

2.2.1.36.3 - Deve sincronizar as assinaturas de IPS, Antivírus, *Anti-Spyware* (ou *antimalware*) quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo.

2.2.1.36.4 - Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e *Anti-spyware* ou *antimalware*: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar *reset* ou tcp-*reset*.

2.2.1.36.5 - Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2.

2.2.1.36.6 - As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

2.2.1.36.7 - Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

2.2.1.36.8 - Deve suportar granularidade nas políticas de IPS, Antivírus e *Anti-Spyware* (ou *antimalware*), possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

2.2.1.36.9 - Deve permitir o bloqueio de vulnerabilidades.

2.2.1.36.10 - Deve permitir o bloqueio de *exploits* conhecidos.

2.2.1.36.11 - Deve incluir proteção contra ataques de negação de serviços.

2.2.1.36.12 - Deverá possuir os seguintes mecanismos de inspeção de IPS:

a) Análise de padrões de estado de conexões;
b) Análise de decodificação de protocolo;
c) Análise para detecção de anomalias de protocolo;
d) IP Defragmentation;
e) Remontagem de pacotes de TCP;
f) Bloqueio de pacotes malformados.

2.2.1.36.13 - Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood e UDPfloof.

2.2.1.36.14 - Detectar e bloquear a origem de *portscans* com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da instituição.

2.2.1.36.15 - Bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões.

2.2.1.36.16 - Possuir tecnologia ou assinaturas para a mitigação de ataques DoS e DDoS.

2.2.1.36.17 - Possuir assinaturas para bloqueio de ataques de buffer overflow.

2.2.1.36.18 - Deverá possibilitar a criação de assinaturas customizadas pelo órgão.

2.2.1.36.19 - Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS, permitindo a criação de exceções com granularidade nas configurações.

2.2.1.36.20 - Permitir o bloqueio de vírus e *spywares* (ou *malwares*) em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMB ou SMB (NetBios-ssn) e SMTP;

2.2.1.36.20.1 - É permitido uso de *appliance* externo (antivírus de rede), para o bloqueio de vírus e **spywares** em protocolo SMB de forma a conter *malwares* se espalhando horizontalmente pela rede.

2.2.1.36.21 - Suportar bloqueio de arquivos por tipo.

2.2.1.36.22 - Deve estar apto a identificar e bloquear comunicação com botnets.

2.2.1.36.23 - Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst.

2.2.1.36.24 - Registrar na console de monitoração as seguintes informações sobre ameaças identificadas.

2.2.1.36.24.1 - O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

2.2.1.36.25 - Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e *Anti-spyware*.

2.2.1.36.26 - Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 ou IPv6), previamente definidos.

2.2.1.36.27 - Os eventos devem identificar o país de onde partiu a ameaça.

2.2.1.36.28 - Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

2.2.1.36.29 - Rastreamento de vírus em pdf.

2.2.1.36.30 - Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo *deflate* (zip, gzip, etc.).

2.2.1.36.31 - Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do *firewall* considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de *firewall* poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

2.2.1.37 - Análise de *malwares*

2.2.1.37.1 - Devido aos *Malwares* hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de *Malwares* não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.

2.2.1.37.2 - O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise *"In Cloud"* ou local, onde o arquivo será executado e simulado em ambiente controlado.

2.2.1.37.3 - A solução deve ser capaz de selecionar por meio de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

2.2.1.37.4 - Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos duas das três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis (como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.).

2.2.1.37.5 - Suportar a análise com pelo menos 50 (cinquenta) tipos de comportamentos maliciosos para a análise da ameaça não conhecida.

2.2.1.37.6 - Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional *Windows* 7 e *Windows* 10;

2.2.1.37.7 - Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, HTTP e SMTP).

2.2.1.37.8 - A solução deve possuir a capacidade de analisar em *sandbox links* (http e HTTPs) presentes no corpo de e-mails trafegados em SMTP. Deve ser gerado um relatório caso a abertura do link pela *sandbox* o identifique como site hospedeiro de *exploits*.

2.2.1.37.9 - Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos *e-mails* permitindo identificação ágil do usuário vítima do ataque.

2.2.1.37.10 - O sistema de análise *"In Cloud"* ou local deve prover informações sobre as ações do *Malware* na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *Malware,* gerar assinaturas de Antivírus e *Anti-spyware* automaticamente, definir URLs não confiáveis utilizadas pelo novo *Malware* e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede).

2.2.1.37.11 - Deve permitir o download dos *malwares* identificados a partir da própria interface de gerência.

2.2.1.37.12 - Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de *malwares* de dia zero.

2.2.1.37.13 - Caso a solução de análise de *malware* seja fornecida em *appliance* local, deve possuir, no mínimo, 25 ambientes controlados *(sandbox)* independentes para execução simultânea de arquivos suspeitos.

2.2.1.37.14 - Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado *(sandbox),* as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante.

2.2.1.37.15 - Suportar a análise de arquivos executáveis, ZIP e criptografados em SSL no ambiente controlado.

2.2.1.37.16 - Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos Java (.jar), Linux (ELF), RAR e 7-ZIP no ambiente de *sandbox*;

2.2.1.37.17 - Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

2.2.1.38- Filtro de URL

2.2.1.38.1 - A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL.

2.2.1.38.1.1 - Permite especificar políticas por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.2.1.38.1.2 - Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.

2.2.1.38.1.3 - Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs por meio da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

2.2.1.38.1.4 - Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

2.2.1.38.1.5 - Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

2.2.1.38.1.6 - Suportar base ou cache de URLs local no *appliance*, evitando **delay** de comunicação/validação das URLs.

2.2.1.38.1.7 - Possui pelo menos 50 categorias de URLs.

2.2.1.38.1.8 - Deve classificar o nível de risco de URLs ou aplicações em, pelo menos, três níveis: baixo, médio e alto.

2.2.1.38.1.9 - A categorização de URL deve analisar toda a URL e não somente até o nível de diretório.

2.2.1.38.1.10 - Permitir a criação categorias de URLs customizadas.

2.2.1.38.1.11 - Permitir a exclusão de URLs do bloqueio, por categoria.

2.2.1.38.1.12 - Permite a customização de página de bloqueio.

2.2.1.38.1.13 - Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site).

2.2.1.38.1.14 - Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

2.2.1.39- Identificação de usuários

2.2.1.39.1 - Deve ser capaz de criar políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, *Active Directory* e base de dados local.

2.2.1.39.2 - 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.

2.2.1.39.3 - Deve possuir integração com *Radius* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

2.2.1.39.4 - Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

2.2.1.39.4.1 - Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x ou soluções NAC via syslog ou radius, para a identificação de endereços IP e usuários.

2.2.1.39.5 - Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no *firewall* (*Captive* Portal).

2.2.1.39.6 - Suportar a autenticação *Kerberos*.

2.2.1.39.7 - Deve suportar autenticação via *Kerberos* para administradores da plataforma de segurança, *Captive* Portal e usuário de VPN SSL;

2.2.1.39.8 - Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estao nestes serviços.

2.2.1.39.9 - Deve implementar a criação de grupos customizados de usuários no *firewall,* baseado em atributos do LDAP/AD;

2.2.1.39.10 - Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente.

2.2.1.40 - QoS

2.2.1.40.1 - Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como *youtube, ustream*, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de

aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*.

2.2.1.40.2 - Suportar a criação de políticas de QoS por:

a) Endereço de origem;
b) Endereço de destino;
c) Por usuário e grupo do LDAP/AD;
d) Por aplicações, incluindo, mas não limitado a *Skype, Bittorrent* e *Youtube*;
e) Por porta.
f) O QoS deve possibilitar a definição de limite de *Upload e Download* ou de classes por: banda garantida, banda máxima e fila de prioridade.

2.2.1.40.3 - Suportar a limitação de upload e download ou a priorização *Real Time* de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

2.2.1.40.4 - Disponibilizar estatísticas *Real Time* para classes de QoS.

2.2.1.40.5 - Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

2.2.1.41 - Filtro de dados

2.2.1.41.1 - Permitir a criação de filtros para arquivos e dados pré-definidos.

2.2.1.41.2 - Os arquivos devem ser identificados por extensão e assinaturas.

2.2.1.41.3 - Permitir a identificação e opcionalmente prevenir a transferência de vários tipos de arquivos (*Office*, PDF, etc.) identificados sobre aplicações (P2P, *Instant Messaging* etc.).

2.2.1.41.4 - Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

2.2.1.41.5 - Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

2.2.1.41.6 - Permitir listar o número de aplicações suportadas para controle de dados.

2.2.1.41.7 - Permitir listar o número de tipos de arquivos suportados para controle de dados.

2.2.1.42 - Geo-localização

2.2.1.42.1 - Suportar a criação de políticas por Geo-localização, permitindo que o tráfego de determinado Pais/Países seja bloqueado.

2.2.1.42.2 - Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

2.2.1.42.3 - Deve possibilitar a criação de regiões geográficas, caso a solução ofertada não possua as regiões pré-cadastradas, e criar políticas utilizando as mesmase criar políticas utilizando as mesmas.

2.2.1.43 - VPN IPSEC/SSL

2.2.1.43.1 - Suportar VPN Site-to-Site e Cliente-To-Site.

2.2.1.43.2 - Suportar IPSec VPN.

2.2.1.43.3 - Suportar SSL VPN.

2.2.1.43.4 - A VPN IPSec deve suportar:

a) DES e 3DES;
b) Autenticação MD5 e SHA-1;
c) *Diffie Hellman Group* 1, *Group* 2, *Group* 5 e *Group* 14;
d) Algoritmo *Internet Key Exchange* (IKEv1 e v2);
e) AES 128 e 256 (*Advanced Encryption Standard*);
f) Autenticação via certificado IKE PKI.

2.2.1.43.5 - A VPN SSL deve suportar:

2.2.1.43.5.1 - O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

2.2.1.43.5.2 - A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

2.2.1.43.5.3 - Atribuição de endereço IP nos clientes remotos de VPN SSL.

2.2.1.43.5.4 - Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL.

2.2.1.43.5.5 - Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário.

2.2.1.43.5.6 - Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como *proxies*.

2.2.1.43.5.7 - Atribuição de DNS nos clientes remotos de VPN;

2.2.1.43.5.8 - Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-spyware* (ou *antimalware*) e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

2.2.1.43.5.9 - Suportar autenticação via AD/LDAP, certificado e base de usuários local.

2.2.1.43.5.10 - Permitir o estabelecimento de túnel VPN *client-to-site* do cliente a plataforma de segurança, integrando-se com as ferramentas de *Windows-logon*.

2.2.1.43.5.11 - Suportar leitura e verificação de CRL (*certificate revocation list*).

2.2.1.43.5.12 - O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory ou ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

2.2.1.43.5.13 - O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

2.2.1.43.5.14 - Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

a) Após autenticação do usuário na estação;
b) Sob demanda do usuário.

2.2.1.43.5.15 - Deve manter uma conexão segura com o portal durante a sessão.

2.2.1.43.5.16 - O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: *Windows Vista, Windows* 7, *Windows* 8, *Windows* 10, Mac OSx, Android e IOS.

2.2.1.43.5.17 - Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

2.2.1.43.5.18 - Deve possuir mecanismos de checagem de conformidade do dispositivo remoto.

2.2.1.43.5.19 - Para atendimento as funcionalidades de VPN IPSEC/SSL, será permitido a composição com solução de concentrador VPN por meio de *appliance* físico ou virtual desde que a solução proposta seja do mesmo fabricante e não implique em custo ou licença adicional.

2.2.1.44 - Console de gerência e monitoramento

2.2.1.44.1 - Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos *appliances*.

2.2.1.44.2 - O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos *appliances* da plataforma de segurança.

2.2.1.44.3 - Controle sobre todos os *appliances* da plataforma de segurança em uma única console, com administração de privilégios e funções, salvo o concentrador VPN.

2.2.1.44.4 - O gerenciame
nto centralizado deverá ser entregue como *appliance* virtual e deve ser compatível com *VMware ESXi* 6.0 ou superior.

2.2.1.44.5 - Deve permitir controle global de políticas para todos os *appliances* que compõe a plataforma de segurança.

2.2.1.44.6 - Deve suportar organizar os *appliances* administrados em grupos: os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição.

2.2.1.44.7 - Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de *firewalls*.

2.2.1.44.8 - Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais *firewalls* e grupos de *firewalls* o usuário terá acesso referente a logs e relatórios.

2.2.1.44.9 - Deve permitir a criação de objetos.

2.2.1.44.10 - Deve consolidar logs e relatórios de todos os *appliances* dispositivos administrados.

2.2.1.44.11 - Deve permitir que exportar backup de configuração automaticamente via agendamento.

2.2.1.44.12 - Deve permitir que a configuração ou pacote de atualização de versão dos *firewalls* seja importada de forma automática, ou manual, na plataforma de

gerenciamento centralizado e que possa ser usada em outros *firewalls* e grupos *de firewalls*.

2.2.1.44.13 - Deve mostrar os status dos *firewalls* em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

2.3.1.44.14 - Deve centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

2.2.1.44.15 - O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

2.2.1.44.16 - Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do *firewall* como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa.

2.2.1.44.17 - Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais *Windows*.

2.2.1.44.18 - O gerenciamento deve permitir/possuir:

a) Criação e administração de políticas de *firewall* e controle de aplicação;
b) Criação e administração de políticas de IPS, Antivírus e *Anti-Spyware* ou *Antimalware*;
c) Criação e administração de políticas de Filtro de URL;
d) Monitoramento de logs;
e) Ferramentas de investigação de logs;
f) Debugging;
g) Captura de pacotes.

2.2.1.44.19 - Acesso concorrente de administradores.

2.2.1.44.20 - Deve permitir que administradores concorrentes façam modificações, validem e/ou revertam configurações do *firewall* simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador.

2.2.1.44.21 - Deve mostrar ao administrador do *firewall* a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.

2.2.1.44.22 - Deve possuir mecanismo busca global na solução onde possa se consultar, por uma *string*, elementos como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas e endereços IPs. Permitindo a localização e uso dos mesmos na configuração do dispositivo.

2.2.1.44.23 - Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

2.2.1.44.24 - Deve permitir monitorar via SNMP falhas de hardware e o uso de recursos do equipamento.

2.2.1.44.25 - Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores.

2.2.1.44.26 - Permitir a definição de perfis de acesso à console com permissões granulares como: acesso de escrita e acesso de leitura.

2.2.1.44.27 - Efetuar a autenticação integrada ao *Microsoft Active Directory* e servidor *Radius*.

2.2.1.44.28 - Permitir efetuar buscas para localizar em quais regras um endereço IP, IP *Range, subnet* ou objetos estão sendo utilizados.

2.2.1.44.29 - Deve atribuir sequencialmente um número a cada regra de *firewall*, NAT e QoS.

2.2.1.44.30 - Permitir a criação de regras que fiquem ativas em horário definido.

2.2.1.44.31 - Permitir a criação de regras com data de expiração.

2.2.1.44.32 - Efetuar *backup* das configurações e *rollback* de configuração para a última configuração salva.

2.2.1.44.33 - Permitir o *Rollback* de Sistema Operacional para a última versão local.

2.2.1.44.34 - Permitir o upgrade via SCP ou interface de gerenciamento.

2.2.1.44.35 - Permitir a validação regras antes da aplicação.

2.2.1.44.36 - Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros.

2.2.1.44.36.1 - Caso necessário, será aceito o uso de *appliance* externo para permitir a validação de regras antes da aplicação.

2.2.1.44.37 - Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

2.2.1.44.38 - Deve possibilitar a integração com a solução de SIEM em uso no TRE-PR, QRadar.

2.2.1.44.39 - Deve gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

2.2.1.44.40 - Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede.

2.2.1.44.41 - Emitir relatórios em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

2.2.1.44.42 - Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, *Antimalware* ou Antivírus e *Anti-spyware*), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes.

2.2.1.44.43 - Deve permitir a criação de *Dash-Boards* customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, *anti-spyware* (ou *anti-malware*), *malwares "Zero Day"* detectados em *sandbox* e tráfego bloqueado.

2.2.1.44.44 - O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.

2.2.1.44.45 - Dever permitir a visualização dos *logs* de *malwares* modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, *anti-spyware* (ou *anti-malware*), Filtro de URL e filtro de arquivos.

2.2.1.44.46 - Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e *Anti-spyware* ou *Anti-malware*), etc..

2.2.1.44.47 - Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), e URLs que passaram pela solução.

2.2.1.44.48 - Deve possuir mecanismo "*Drill-Down*" para navegação nos relatórios em *Real Time*.

2.2.1.44.49 - Nas opções de *"Drill-Down"*, ser possível identificar o usuário que fez determinado acesso.

2.2.1.44.50 - Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de *malwares* por meio de aplicativos SaaS com a informação do usuário responsável pelo acesso.

2.2.1.44.51 - Permitir a rotação dos logs.

2.2.1.44.52 - Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado.

2.2.1.44.53 - Exibição das seguintes informações, de forma histórica e em tempo real:

a) Situação do dispositivo e do cluster;
b) Principais aplicações;
c) Administradores autenticados na gerência da plataforma de segurança;
d) Status das interfaces;
e) Uso de CPU;

2.2.1.44.54 - No mínimo os seguintes relatórios devem ser gerados:

a) Resumo gráfico de aplicações utilizadas;
b) Principais aplicações por utilização de largura de banda de entrada e saída;
c) Principais aplicações por taxa de transferência de bytes;
d) Principais hosts por número de ameaças identificadas;
e) Atividades de um usuário específico do AD/LDAP, incluindo aplicações acessadas, categorias de URL, e ameaças (IPS, Antivírus e *Anti-spyware* ou *anti-malware*), de rede vinculadas a este tráfego;
f) Deve permitir a criação de relatórios personalizados.

2.2.1.44.55 - Gerar alertas automáticos via, pelo menos, por e-mail e SNMP.

2.2.1.44.56 - A plataforma de segurança deve permitir através de API (*Application Program Interface*) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em Real Time com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

2.2.1.44.57 - Para comprovação de atendimento aos requisitos técnicos previstos neste termo **não** serão aceitas declarações e/ou cartas de fabricantes ou licitantes. Serão considerados os documentos de domínio público dos respectivos equipamentos

e softwares. Caso a documentação de domínio pública seja omissa ou dúbia, poderá ser solicitada amostra para comprovação do atendimetno das características (conforme item 9 do edital).

2.2.1.44.58 - Os equipamentos ofertados devem obrigatoriamente ter certificação da ANATEL.

2.2.1.44.59 - Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a de capacidade ilimitada.

2.2.1.44.60 - Caso a solução possua módulo de relatórios estendida, deverá ser entregue junto com a solução.

2.2.1.44.61 - As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 36 (trinta e seis) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu uso.

2.2.1.44.62 - Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em até 3 (três) dias úteis, para todos os componentes da solução.

2.2.2 - Do suporte técnico durante a garantia contratual:

2.2.2.1 - Durante o período de Garantia, a CONTRATADA deverá prestar suporte técnico, atender às solicitações do TRE-PR, efetuadas pela Seção de Rede, respeitando as condições e níveis de serviço especificados a seguir;

2.2.2.2 - A severidade dos chamados de suporte e garantia serão determinadas conforme este contrato e o prazo de atendimento será contado a partir da abertura de ordem de serviço e será classificado conforme as severidades especificadas a seguir;

2.2.2.3 - Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade de componentes da solução ou as aplicações que são acessadas por meio da solução estão indisponíveis.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 horas	12 horas	08 horas	16 horas

2.2.2.4- Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha no uso da solução, estando ainda disponível, porém apresentando problemas ou instabilidade.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
06 horas	48 horas	10 horas	48 horas

2.2.2.5 - Severidade BAIXA: Esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso da solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.

Dias úteis		Sábados, domingos e feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
30 horas	72 horas	-	-

2.2.2.6 - Serão considerados para efeitos dos prazos exigidos:

2.2.2.6.1 - Prazo de Atendimento: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e o efetivo início dos trabalhos de manutenção.

2.2.2.6.2 - Prazo de Solução Definitiva: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do TRE-PR à Prestadora de Serviço e a efetiva recolocação dos equipamentos em seu pleno estado de funcionamento e operação normais.

2.2.2.7 - A contagem do prazo de atendimento e solução definitiva de cada solicitação será a partir da notificação à contratada, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica do TRE-PR;

2.2.2.8 - O atendimento às solicitações de severidade ALTA deverá ser realizado nas instalações da TRE-PR (on-site) e não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderá implicar em custos adicionais ao TRE-PR. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte da contratada e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar na aplicação das sanções previstas neste contrato.

2.2.2.9 - As ordens de serviços classificadas com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escaladas para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como sanções previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte da contratada e que não tenha sido previamente autorizado pelo TRE-PR, poderá ensejar na aplicação das sanções previstas neste contrato.

2.2.2.10- Depois de concluído o suporte técnico, o licitante vencedor comunicará o fato à Equipe Técnica do TRE-PR e solicitará autorização para o fechamento do chamado. Caso o TRE-PR não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela contratada. Nesse caso, o TRE-PR fornecerá as pendências relativas à solicitação em aberto.

2.2.2.11- O TRE-PR encaminhará a contratada, quando da reunião de apresentação inicial, relação nominal da equipe técnica autorizada a abrir e fechar solicitações de suporte técnico.

2.2.2.12 - Por necessidade excepcional de serviço, o TRE-PR também poderá solicitar a escalação de chamado para níveis superiores de severidade. Nesse caso, a escalação deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

CLÁUSULA TERCEIRA: DAS OBRIGAÇÕES DA CONTRATADA

3.1 – Da entrega:

3.1.1 – Do prazos:

3.1.1.1 – **Prazo de entrega da solução:** a solução deverá ser entregue em um prazo de até **60 (sessenta) dias corridos**, a contar da assinatura do contrato.

3.1.1.2 – **Prazo de instalação e configuração**: a solução deverá ser instalada e configurada em um prazo de até **60 (sessenta) dias corridos**, contados da data de recebimento provisório.

3.1.2 – **Do local de entrega:** a solução deverá ser entregue no Tribunal Regional Eleitoral do Paraná, Rua João Parolin, nº 224, Curitiba-PR, Seção de Rede, agendamento pelos telefones (41) 3330-8628 ou 3330-8629.

3.2 – Do recebimento do objeto:

3.2.1 – **Do recebimento provisório:** em até 10 (dez) dias corridos a solução será recebida, provisoriamente, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência.

3.2.2 – O recebimento provisório será realizado pela Seção de Gestão de Equipamentos de Microinformática.

3.2.3 - Na hipótese de constatação de anomalias que comprometam a utilização adequada da solução, ela será rejeitada, em todo ou em parte, conforme dispõe o Art. 76 da Lei n° 8.666/93, sem qualquer ônus para o TRE-PR, devendo o licitante vencedor reapresentá-la (s) no prazo máximo de até 30 (trinta) dias, após o comunicado.

3.2.4 – **Do recebimento definitivo: a** verificação da conformidade das especificações da solução ocorrerá no prazo de até 10 (vinte) dias corridos, contados a partir do recebimento provisório. Atestada a conformidade quantitativa e qualitativa, a solução será recebida definitivamente.

3.2.4.1- O recebimento definitivo será realizado pela Coordenadoria de Infraestrutura.

3.3 – Da garantia:

3.3.1 - A solução ofertada deverá estar coberta por garantia total fornecida pelo fabricante, pelo prazo de **36 (trinta e seis) meses.**

3.3.1.1 - A garantia iniciará a partir da data de recebimento definitivo da solução.

3.3.2 - A contratada deverá apresentar o Certificado de Garantia emitido pelo fabricante, no prazo de até 30 (trinta) dias corridos, a contar da data de recebimento definitivo da solução.

3.3.3 - A contratada deverá possibilitar a abertura de chamado técnico diretamente no fabricante da solução ou por centro de suporte devidamente autorizado pelo fabricante.

3.3.4 - O atendimento de primeiro nível deve ser realizado em português do Brasil.

3.3.5 - Deve ser disponibilizado pelo menos um dos seguintes canais de atendimento para suporte:

a) Telefone 0800;
b) Sistema Web de abertura de chamados;
c) E-mail.

3.3.6 - A Contratada deverá disponibilizar o acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações de assistência, orientação para instalação, desinstalação, configuração, atualização de *firmware e software*, aplicação de correções (patches), diagnóstico, avaliações e resolução de problemas, e demais atividades relacionadas à correta operação, e funcionamento da solução.

3.3.7 – A Contratada deverá, semestralmente, revisar as atualizações de drivers, firmwares e microcódigos de todos os *appliances* contratados. Os serviços de atualizações de *firmwares* somente deverão ocorrer para os eventos classificados como críticos.

3.3.8 - Os serviços cobertos pela garantia deverão ser prestados nas instalações do TRE-PR, em Curitiba/PR.

3.3.9 - Os serviços cobertos pela garantia deverão ser prestados pela empresa fabricante, pela contratada ou parceiro autorizado/credenciado, através da disponibilização de técnicos certificados pelo fabricante da solução.

3.3.10 - A Contratada deverá fornecer a seus técnicos as ferramentas e instrumentos necessários à execução dos serviços, bem como produtos ou materiais indispensáveis à manutenção do equipamento.

3.3.11 - Os discos rígidos que forem substituídos ou no caso de troca de equipamento ficarão retidos e serão de propriedade do TRE-PR.

3.3.12 - A Contratada deverá garantir atualizações do produto e suporte técnico do fabricante (telefone, e-mail ou acesso remoto) pelo período de vigência da garantia.

3.3.13 - A substituição de equipamento defeituoso deverá ocorrer em até 30 (trinta) dias corridos, após a abertura de Ordem de Serviço pelo gestor de contrato ou notificação automática do sistema na central de atendimento do licitante vencedor ou fabricante.

3.4 – A Contratada deverá apresentar, ao gestor da contratação, em até 30 (trinta) dias corridos contados da assinatura do contrato, no momento da entrega dos equipamentos, os documentos abaixo:

a) Certificação/declaração emitida pelo fabricante do equipamento ofertado (ou credenciado) para, no mínimo, 02 (dois) funcionários, atestando participação em curso/treinamento específico relacionado à utilização/configuração/suporte do equipamento ofertado.

b) Comprovação do vínculo dos funcionários certificados (conforme alínea a) com a empresa contratada, mediante apresentação de carteira profissional ou contrato de prestação de serviços.

3.5 – Da sustentabilidade:

3.5.1 Será exigida a compatibilidade do produto com a diretiva RoHS (RoHS Restriction of Certain Hazardous Substances ou Restrição de Certas Substâncias Perigosas), a qual limita a um percentual máximo o uso de substâncias perigosas nos processos de fabricação dos produtos, entre elas: cádmio (Cd), mercúrio (Hg), cromo hexavalente (CrVI), bifenilos polibromados (PBBs), éteres difenil-polibromados (PBDEs) e chumbo (Pb), de modo a contribuir para a redução do impacto ambiental.

3.5.2 - Os produtos deverão ser preferencialmente, acondicionados em embalagem individual adequada, com menor volume possível, que utilize materiais recicláveis, de

forma a garantir a máxima proteção durante o transporte e o armazenamento. As condições deste item serão objeto de verificação *in loco* no momento da entrega dos produtos.

3.6 - A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

CLÁUSULA QUARTA: DA DESPESA ORÇAMENTÁRIA

4.1 – Os recursos serão destinados à contratação conforme abaixo:

Programa de Trabalho: 02122057020GP0041;
Nota de Empenho: 2019NE001845, emitida em 17/12/2019;
Elemento de despesa: 44.90.52.37;
Categoria Econômica: Investimentos;
Código SIASG: BR0150100

CLÁUSULA QUINTA: DA VIGÊNCIA

5.1 - O presente contrato vigorará pelo período de **39 (trinta e nove) meses,** a partir da data da assinatura, **de 08/01/2020 a 07/04/2023,** podendo ser rescindido antecipadamente a critério do CONTRATANTE, nos termos da Lei nº 8.666/93.

CLÁUSULA SEXTA: DO REAJUSTE

6.1 - Os preços não serão reajustáveis, tendo em vista tratar-se de contrato de garantia contratual.

CLÁUSULA SÉTIMA: DO PAGAMENTO

7.1 - O valor total a ser pago à CONTRATADA, pelo cumprimento do objeto deste contrato será de **R$ 360.000,00 (trezentos e sessenta mil reais)**, conforme item a seguir especificado:

	Item	Descrição	Quantidade	Valor Unitário	Valor total
LOTE 1	1	*Appliance Next Generation Firewall (NGFW)*, com interface de gerência e respectivas licenças, garantia, suporte e atualizações por 36 meses	2	R$ 180.000,00	R$ 360.000,00

7.2 – Do documento fiscal:

7.2.1 – O documento fiscal deverá atender os requisitos abaixo, podendo ser emitido na forma eletrônica - NOTA FISCAL ELETRÔNICA, nos termos da legislação vigente, devendo ser encaminhado ao gestor do contrato do TRE/PR por e-mail, em formato PDF ou emitido na forma física devendo ser encaminhado a Seção de Protocolo, localizada na Rua João Parolin, 224, 1º andar, Curitiba/Paraná.

7.2.1.1 – O CNPJ cadastrado no sistema comprasnet/documentos de habilitação, deverá ser o mesmo para efeito de emissão da nota fiscal/fatura para posterior pagamento.

7.2.1.2 - Caso a CONTRATADA não possa emitir a nota fiscal/fatura com o mesmo CNPJ habilitado na licitação, poderá fazê-lo através da eventual matriz ou filial da mesma empresa licitante vencedora. Nesse caso, ambos os CNPJs (CONTRATADA e eventual matriz ou filial utilizada) deverão estar com a documentação fiscal regular e atender obrigatoriamente os seguintes requisitos:

- CNPJ da CONTRATADA
- CNPJ do TRE: 03.985.113/0001-81;
- Data de emissão da nota fiscal;
- Descritivo dos valores unitários e totais,
- Número do contrato
- Banco
- Agência
- Número da conta corrente (obrigatoriamente da própria CONTRATADA)

7.3 – Das condições do pagamento:

7.3.1 - O pagamento somente ocorrerá depois de atestado pelo gestor do contrato designado para esta finalidade. O atestado será realizado, obedecendo o prazo e formulário específico, conforme dispositivos legais deste TRE/PR.

7.3.2 - O pagamento será efetuado mediante crédito em conta corrente, conforme indicação da CONTRATADA no documento fiscal, por intermédio de ordem bancária, de acordo com os seguintes prazos:

7.3.2.1 – Prazo para atestado da Nota fiscal: **até 05 (cinco) dias úteis** a partir do aceite da nota fiscal pelo gestor, a qual deverá ser enviada pela empresa somente após cumpridas todas as exigências contratuais.

7.3.2.1.1 - A Nota Fiscal/Fatura, após o atestado do gestor da contratação, será encaminhada à Secretaria de Orçamento, Finanças e Contabilidade, para que se efetive o pagamento.

7.3.2.2 – Prazo para pagamento da Nota Fiscal: **até 20 (vinte) dias corridos** após o atestado da Nota fiscal pelo Gestor.

7.3.2.2.1 - Se o valor da nota fiscal for de até R$ 17.600,00 (dezessete mil e seiscentos reais), o prazo para pagamento será de **05 (cinco) dias úteis** após o atestado realizado pelo fiscal da contratação, conforme o disposto no art. 5º, § 3º da Lei nº 8.666/93.

7.3.3 – Será considerado como data do pagamento, o dia em que constar como emitida a ordem bancária para pagamento.

7.3.4 – O gestor da contratação do TRE/PR procederá à conferência dos requisitos da nota fiscal/fatura, que deverá estar de acordo com as descrições contidas na nota de empenho, bem como apresentar o mesmo número de CNPJ cadastrado, habilitado e constante nos documentos entregues, não se admitindo notas fiscais/faturas emitidas com outro CNPJ, salvo na hipótese prevista no item 7.2.1.2.

7.3.4.1 – Havendo erro na apresentação do documento fiscal ou dos documentos pertinentes à contratação, ou ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará pendente até que a CONTRATADA providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação, não acarretando qualquer ônus para o TRE/PR.

7.3.5 – O TRE/PR, observados os princípios do contraditório e da ampla defesa, poderá deduzir, do montante a pagar à CONTRATADA, acréscimos decorrentes de mora no

recolhimento de tributos/contribuições, bem como de multa decorrente de previsão deste edital e/ou anexo(s).

7.3.6 – DA ATUALIZAÇÃO MONETÁRIA: Na ocorrência de eventual atraso de pagamento e, desde que a CONTRATADA não tenha concorrido para tanto, serão devidos encargos moratórios pelo TRE/PR, entre a data prevista para o pagamento e a do efetivo pagamento, mediante solicitação formal do interessado, que serão calculados por meio da aplicação da fórmula EM = I x N x VP, onde:

EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso

I = Índice de compensação financeira = 0,00016438, assim apurado:
I = i/365 (onde i = taxa percentual anual no valor de 6%)
I = (6/100)/365

7.4 – Da regularidade fiscal:

7.4.1 – Todo e qualquer pagamento, decorrente da presente contratação, será precedido de verificação, por parte do TRE/PR, da regularidade fiscal da CONTRATADA em vigor na data do pagamento.

7.4.1.1 – A CONTRATADA inadimplente quanto à regularidade fiscal estará sujeita à abertura de processo administrativo pelo Gestor da contratação do TRE/PR, visando à regularização.

7.4.1.1.1 – Permanecendo a inadimplência poderá haver rescisão contratual, independentemente da aplicação das sanções previstas neste edital e/ou anexo(s).

7.4.2 – A regularidade de que trata o subitem anterior poderá ser verificada:

a) por meio de consulta on-line no Sistema de Cadastramento Unificado de Fornecedores – SICAF e/ou;
b) por meio de consulta aos sites oficiais e/ou;
c) por meio da apresentação de documentação, pela CONTRATADA, anexada ao documento fiscal.

7.4.2.1 – O resultado das consultas, de que trata as alíneas acima, serão realizadas pelo setor financeiro responsável e deverão constar do processo de pagamento.

CLÁUSULA OITAVA: DA SUBSTITUIÇÃO TRIBUTÁRIA

8.1 – Da substituição tributária:

8.1.1 - Serão feitas as retenções tributárias federais e municipais incidentes sobre a contratação, conforme artigo 64 da Lei nº 9.430/96, IN RFB 1234/12, IN RFB 971/09, LC nº 116/2003 e LC nº 123/06, conforme o objeto da contratação.

8.2 – Dos tributos federais:

8.2.1 - Será efetuada a retenção dos tributos federais aplicando-se, sobre o valor a ser pago, o percentual constante da Tabela de Retenção da IN RFB 1234/12.

8.2.2 - Quando a empresa for optante do Regime Simplificado Nacional (SIMPLES), não haverá a retenção de que trata o item acima.

8.2.3 - A nota fiscal, cuja empresa CONTRATADA seja Optante do SIMPLES, deverá estar acompanhada da Declaração, nos termos do caput do artigo 6º da IN RFB 1234/12 - anexo IV.

8.3 - Da retenção previdenciária:

8.3.1 - Quando o objeto da contratação contemplar cessão de mão de obra ou empreitada, poderá ocorrer a retenção do INSS prevista no artigo 112, sobre os serviços elencados nos artigos 117 e 118 da IN RFB 971/09.

8.4 - Da retenção do ISS:

8.4.1 - Sobre serviços, poderá ocorrer a retenção do ISS, quando o objeto da contratação se enquadrar no inciso II, do § 2º do art.6º da LC nº 116/03.

8.4.2 - Quando a empresa for optante do Regime Simplificado Nacional (SIMPLES) deverá destacar na nota fiscal de prestação de serviços a alíquota na qual está enquadrada, conforme os anexos III ou IV da Lei Complementar nº 123/06. Caso não haja o referido destaque, será considerada a alíquota máxima vigente, ou seja, 5% (cinco por cento).

8.5 - Quanto à incidência das retenções de tributos prevalecerá sempre a legislação vigente, mesmo que venham a contrariar as disposições acima, conforme sua incidência ou não sobre o objeto contratado.

8.6 - A atualização monetária e a multa, provenientes do atraso no recolhimento das obrigações tributárias e/ou previdenciárias serão descontadas do valor da Nota Fiscal/Fatura correspondente, quando a CONTRATADA lhes der causa.

8.6.1 - O não atendimento às especificações do documento fiscal, descritas na cláusula sétima, item 7.2, bem como a não comprovação da regularidade fiscal, prevista na cláusula sétima, item 7.4.1, darão causa ao previsto no item anterior.

CLÁUSULA NONA: DOS GESTORES DO CONTRATO

9.1 - O fornecimento será acompanhado pelo Chefe da Seção de Rede e seu substituto, que serão os gestores da contratação.

9.2 - Nos termos da Lei nº 8666/93, art. 67, parágrafos 1º e 2º, caberá aos Gestores:

a) receber e atestar a nota fiscal referente à aquisição, encaminhando a fatura pertinente ao setor responsável pelo tombamento dos bens e, seguidamente, à Secretaria de Orçamento, Finanças e Contabilidade do TRE/PR, para pagamento;

b) acompanhar o fornecimento de acordo com as condições contratadas, determinando o que for necessário para regularização das faltas ou defeitos observados, sob pena de responsabilização administrativa;

c) se a inexecução persistir, o gestor deverá criar um Processo Administrativo Digital (PAD) específico e encaminhá-lo à Secretaria de Gestão Administrativa, devidamente instruído com todas as informações pertinentes constantes de formulário específico, anexando-se cópia(s) do(s) e-mail(s) relativos ao item anterior (letra "b"), referente(s) à intenção de abertura de Processo Administrativo, com o respectivo comprovante de recebimento pela Contratada.

CLÁUSULA DÉCIMA: DAS SANÇÕES ADMINISTRATIVAS

10.1 - O descumprimento de quaisquer das obrigações descritas no presente instrumento poderá ensejar abertura de processo administrativo, garantido o contraditório e a ampla defesa, de acordo com o capítulo IV, art. 87 da Lei nº 8666/93 e artigo 7º da lei nº 10520/2002:

10.2 – Poderão ser aplicadas ainda as seguintes sanções:

a) Advertência;

b) Multas:

b.1) Multa de 1,0% (um por cento) ao dia sobre o valor contratado, pelo atraso no cumprimento ao prazos de entrega estipulado no presente instrumento, com limite de 10 (dez) dias. Após esse prazo, será considerado inadimplemento parcial, com multa de 15% (quinze por cento) sobre o valor total do contrato;

b.2) Multa de 5,0% (cinco por cento) sobre o valor total da contratação pelo inadimplemento a quaisquer outras obrigações pactuadas, e que venham a causar prejuízos o CONTRATANTE, independente do ressarcimento dos danos à Administração.

b.3) Na prestação da Garantia Técnica, estará sujeita às sanções abaixo, pelos descumprimentos dos prazos previstos para solucionar os chamados de SUPORTE TÉCNICO, nos termos previstos no item 2.3 deste contrato, conforme abaixo:

Sanção	Classificação
0,05 % por dia de atraso, limitado a 30 dias, sobre o valor total do contrato.	Severidade alta
0,02% por dia de atraso, limitado 30 dias, sobre o valor total do contrato.	Severidade média
0,01% por dia de atraso, limitado a 30 dias, sobre o valor total do contrato.	Severidade baixa

b.4) Multa de 10% (dez por cento) sobre o valor total do contrato, pela não prestação da garantia dos equipamentos e/ou serviços fornecidos dentro dos prazos previstos em contrato e/ou no Código de Defesa do Consumidor; ou pela ocorrência de quaisquer danos aos equipamentos, ocasionados por negligência ou imperícia dos profissionais, sem a reposição ou conserto imediato do bem pertinente;

b.5) Multa de 15% (quinze por cento) sobre o valor total do contrato, pela não atendimento a qualquer chamado feito pelo CONTRATANTE para manutenção e correção de problemas ou pela inadimplência reiterada das obrigações pactuadas.

b.6) Multa de 10% (dez por cento) sobre o valor contratual, pelo inadimplemento parcial do contrato;

b.7) Multa de 20% (vinte por cento) sobre o valor contratual, pelo inadimplemento total do contrato;

c) Impedimento de licitar e contratar com a União, conforme previsto no art.7º da Lei nº 10.520/02, bem como o descredenciamento do SICAF, ou dos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/02, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, conforme a gravidade do inadimplemento da obrigação e prejuízos ocasionados, quando a empresa, convocada dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar a documentação exigida ou apresentar documentação falsa para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou

fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.

10.4 - As sanções de advertência e de impedimento de licitar e contratar, previstas nos itens 10.1, 10.2, poderão ser aplicadas, cumulativamente ou não, com a pena de multa.

10.5 - No caso de aplicação de multa determinada em processo administrativo que garanta a ampla defesa à CONTRATADA, esta deverá recolher à União o valor imputado por meio de GRU.

10.6 - As multas imputadas à Contratada cujo montante seja superior ao mínimo estabelecido pelo Ministério da Fazenda[2] e não pagas no prazo concedido pela Administração, serão inscritas em Dívida Ativa da União e cobradas com base na Lei nº 6830/80, sem prejuízo da correção monetária.

CLAUSULA DECIMA PRIMEIRA: DA RESCISAO DO CONTRATO

11.1 - Ficará o presente contrato rescindido, a juízo da administração, mediante formalização, assegurado o contraditório e a ampla defesa, nos casos elencados nos arts. 77 a 80 da Lei nº 8.666/93.

11.2 - Será também causa de rescisão se a Contratada alocar funcionários, para o desempenho dos serviços, que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento de membros ou juízes vinculados a este Tribunal, contrariando o artigo 3º da Resolução nº 07, de 18/10/2005, com redação dada pela Resolução nº 09, de 06/12/05, ambas do CNJ (Conselho Nacional de Justiça).

CLÁUSULA DÉCIMA SEGUNDA: DOS CASOS OMISSOS

12.1 - Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 8.666/93 e, subsidiariamente, na Lei nº 9.784/99, no Código de Defesa do Consumidor e demais normas e princípios gerais aplicáveis.

CLÁUSULA DÉCIMA TERCEIRA: DO FORO

13.1 - Fica eleito o Foro de Curitiba-PR para dirimir as divergências oriundas do presente contrato.

13.2 - E, por estarem assim justas e contratadas, assinam o presente em 02 (duas) vias de igual teor e forma.

Curitiba, 08 de janeiro de 2020.

Patrícia Angelina da Conceição

Patrícia Angelina da Conceição
Representante Legal
P/ CONTRATADA

Valcir Mombach
Diretor-Geral - TRE/PR.
P/ CONTRATANTE

[2] Portaria n.º 75 do Ministério da Fazenda, publicada em 22/03/2012 – artigo 1.º, inciso I.

EM BRANCO

PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

CONTRATO Nº 11/2020
SEI Nº 0004291-41.2020.6.02.8000

CONTRATO CELEBRADO ENTRE A UNIÃO, POR MEIO DO TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS, E A EMPRESA NOVA SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO DE NETWORKING EIRELI EPP, PARA OS FINS QUE ESPECIFICA (Pregão Eletrônico nº. 28/2019 Processo ELETRÔNICO SEI Nº 0005970-17.2019.6.27.8000)

A União, Pessoa Jurídica de Direito Público Interno, por intermédio do **TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS - TRE/AL**, Órgão do Poder Judiciário, situado na Avenida Aristeu de Andrade, nº 377, Farol – CEP 57051-090 - Maceió/AL, inscrito no CNPJ/MF sob o nº 06.015.041/0001-38, neste ato representado por seu Vice-Presidente, no exercício da Presidência, Desembargador Otávio Leão Praxedes, brasileiro, casado, Magistrado, portador da Carteira de Identidade nº 215.430, inscrito no CPF sob o nº 087.912.284-06, residente e domiciliado nesta cidade, doravante denominada CONTRATANTE, e, de outro lado, e a empresa_**NOVA SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E NETWORKING EIRELI EPP**, inscrita no CNPJ/MF nº 10.685.932/0001-79, estabelecida no ST. SRTV/Sul, Quadra 701, Lote 04, Bloco "o", sala 899-A, Ed. Multiempresarial, Asa Sul, CEP 70340-000, Brasília/DF, e-mail administrativo@inovazul.com.br , telefone (61 3032-6602/3703-4444, representada neste ato pelo Sr. José Jacob Nácul, representante legal, brasileiro, portador da Carteira de Identidade 4015908439 SSP/RS, CPF/MF nº 037.236.648-14, doravante denominada CONTRATADA, considerando o julgamento do Pregão Eletrônico Tribunal Regional Eleitoral do Tocantins – TRE/TO nº 28/2019 e a respectiva homologação, celebram o presente Contrato, adesão à Ata de Registro de Preços nº 54/2019 do TRE/TO, observando-se as normas constantes nas Leis n. 8.666/1993 e 10.520/2002, no Decreto nº 5.450/2005, e ainda, mediante as cláusulas a seguir enumeradas.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Constitui objeto do presente contrato a aquisição de atualização da solução de firewall do Tribunal Regional Eleitoral de Alagoas, incluindo o serviços de garantia técnica para o período de 60 (sessenta) meses, observados o Edital, o Termo de Referência e a proposta da Contratada, os quais independentes de transcrição são partes integrantes e serão observados naquilo que não o contrarie.

1. 2 Os itens contratados são os discriminados na tabela abaixo:

PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

ITEM	BENS/SERVIÇO	QUANTIDADE
2	Atualização da Solução de firewall tipo pequeno porte com atualização dos equipamentos Sonicwall TZ 200/205 para no mínimo equivalente ao Sonicwall SOHO Wireless, com serviço de suporte 8x5 cobertos pela Garantia de 60 meses.	25

CLÁUSULA SEGUNDA – DA ESPECIFICAÇÃO TÉCNICA

2.1. A Atualização da Solução de Firewall consiste no seguinte:

2.1.1. Atualização dos atuais equipamentos por meio de Substituição por outros superiores, conforme descritos no Termo de Referência.

2.1.2. Fornecimento de serviços de suporte técnico para solução de eventuais problemas de funcionamento dos equipamentos dos firewalls pelo período de Garantia contratado, incluindo substituições de hardwares quando necessário durante a vigência da Garantia;

2.1.3 .Fornecimento, ativação e manutenção dos requisitos de segurança nos firewalls, conforme descritos no Termo de Referência, pelo período de Garantia contratado;

2.1.4. Diante dos procedimentos legais para desfazimento de Patrimônios Públicos a Contratada ao concordar em participar do Certame, tacitamente já concorda que os equipamentos substituídos serão oportunamente incluídos ao processo administrativo de desfazimento de bens, o que impedirá de retirá-los do Tribunal em ato contínuo à implantação da solução contratada;

2.1.5. Fornecimento dos Serviços de instalação dos novos equipamentos, configuração, migração de todos os objetos e regras de firewall, configuração de VPNs entre firewall concentrador e firewalls de pequeno porte, enfim, todos os serviços para a efetiva migração da solução de firewall do Tribunal até alcançar plena estabilidade operacional;

2.1.6. A retirada dos atuais equipamentos do modo operacional se dará somente com a efetiva instalação e estabilização dos serviços ativos nos novos equipamentos;

2.1.6.1. Caso seja fornecida a Atualização da Solução de Firewall com equipamentos em substituição de outro fabricante, a contratada deverá, SEM CUSTO ADICIONAL, fornecer ao Tribunal treinamento presencial para a equipe de técnicos do Tribunal composta de até 10 (dez) pessoas, podendo o treinamento ser na modalidade “in company”, conforme especificado neste Termo de referência;

2.1.7. A substituição deverá ser por equipamentos novos, podendo ser da mesma família de produção, porém, de mode-

los superiores, de lançamento no mercado em data mais recente dos atuais equipamentos;
2.1.8. Os novos equipamentos deverão estar em linha de produção quando da entrega dos equipamentos para fins de substituição;
2.1.9. Deverá possuir recursos técnicos e desempenho de processamento equivalente ou superior aos atuais equipamentos;
2.1.10. Na tabela a seguir consta os modelos dos atuais equipamentos, bem como os modelos de referência mínimo aceitável, em termos de performance e capacidade de processamento, para fins de substituição:

Item	Modelo atuais equipamentos	Modelo mínimo aceitável como referência técnica para os novos equipamentos
2	Sonicwall TZ 200/205	SonicWall SOHO Wireless

2.2. Especificações técnicas dos novos equipamentos de firewall de pequeno porte (SOHO Wireless ou equivalente) para a solução de firewall.

2.2.1. Para os equipamentos de Firewall de pequeno porte, que tem como modelo mínimo aceitável como referência técnica para os novos equipamentos o equipamento modelo Sonicwall SOHO Wireless ou equivalente/superior de outro fabricante, deverá contemplar os serviços de suporte no mínimo na modalidade 8x5 (oito horas/dia e 5 dias/semana) a serem mantidos durante o período de garantia da Solução Ofertada, que será de 60 meses. O equipamento ofertado deve possuir, no mínimo, as características técnica do modelo de referência, em destaque as seguintes características:

2.2.1.1. Deve possuir no mínimo 5 interfaces 10/100/1000 GbE. Todas operando em modo autosense e em modo half/full duplex, com inversão automática de polaridade configuráveis pelo administrador do firewall para atender os segmentos de segurança e rede para:

- ✓ Segmento WAN , ou externo;
- ✓ Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema;
- ✓ Segmento LAN ou rede interna;
- ✓ Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada);
- ✓ Segmento ou Zona dedicada para controle de dispositivos Wireless dedicado com controle e configuração destes dispositivos.

2.2.1.2. Possuir no Mínimo de 512MB de memória RAM para maior confiabilidade do sistema;
2.2.1.3. A Fonte de alimentação deve ser com operação automática entre 110/220V.

2.2.1.4. Deve possuir no mínimo 01 interface USB com suporte a conexão 3G/4G (Wan Failover);

2.2.1.5. Deve possui controlador Wireless padrão 802.11 a/b/g/n;

2.2.1.6. Possuir Performance de Firewall SPI (Stateful Packet Inspection) igual ou superior a 300 Mbps;

2.2.1.7. Possuir Performance para inspeção de Anti-Malware integrado no mesmo appliance: 150 Mbps ou superior;

2.2.1.8. Possuir capacidade mínima de conexões suportadas em modo firewall de 10.000 Mil conexões;

2.2.1.9. Deve Suportar no mínimo 1.800 novas conexões por segundo;

2.2.1.1.0. Deve Suportar no mínimo 25 interfaces de vlan (802.1q) suportando a definição de seus endereços IP através da interface gráfica;

2.2.1.11. O equipamento deve ter a capacidade de suportar a análise de tráfegos criptografados HTTPS/SSL, onde o mesmo deverá ser descriptografado de forma transparente a aplicação;

2.2.1.12. Possuir Performance de VPN IPSEC (3DES & AES 256) de 100 Mbps ou superior;

2.2.1.3. Deve ter capacidade de Prover servidor DHCP Interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;

2.2.1.1.4. Deve suportar no mínimo 10 túneis VPN IPSEC do tipo site- to-site já licenciadas;

2.2.1.15. Deve suportar no mínimo 5 túneis VPN IPSEC do tipo client- to-site, devendo disponibilizar para cada equipamento no mínimo 01 Licença/conexão, sem custo adicional;

2.2.1.16. Deve Suportar no mínimo 10 conexões clientes do tipo SSL, devendo disponibilizar junto com cada equipamento no mínimo 01 licença/conexão, sem custo adicional;

2.2.1.17. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

2.2.1.18. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication;

2.2.1.19. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

2.2.1.20. Deve permitir utilização de LDAP, AD e RADIUS;
2.2.1.21. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
2.2.1.22. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;
2.2.1.23. Deve ter capacidade de Suportar no mínimo 250 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo;
2.2.1.24. Deve permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
2.2.1.25. Deve possibilitar gerência remota, com interface gráfica nativa;

2.2.1.26. Deve ter capacidade de fornecer interface gráfica para no mínimo 3 usuários;
2.2.1.27. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
2.2.1.28. Os produtos de hardware ofertados devem ser novos, nunca terem sido utilizados e não terem sido descontinuados, ou seja, devem constar na linha atual de comercialização e suporte do fabricante;
2.2.1.29. O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade,

ou seja, de um firewall não sendo baseado em plataforma X86 ou equivalente.

2.3. A CONTRATADA será responsável por todo o processo de ativação dos requisitos de segurança integrantes da solução de firewall, bem como nas demandas de atualização de todos os hardwares contratados, dentre eles: gerar e fornecer os arquivos necessários, executar a renovação/atualização no portal de gerência do fabricante para todos os firewalls, e demais demandas que forem necessárias;

CLÁUSULA TERCEIRA - SERVIÇO DE INSTALAÇÃO/MIGRAÇÃO E TREINAMENTO OFICIAL

3.1. SERVIÇO DE INSTALAÇÃO/MIGRAÇÃO

3.1.1. A Contratada deverá disponibilizar, no prazo constante neste termo, técnicos devidamente certificados junto ao fabricante da solução ofertada para realizar todos os serviços de instalação/migração;

3.1.2. Os técnicos designados para essa missão deverão possuir experiências no processo de implantação de solução de firewall;

3.1.3. Toda a configuração existente em termos de enlace de redes, VPNs, rotas, objetos e regras de firewalls, etc., deverão ser migrados para nova solução ofertada;

3.1.4. Todos os serviços serão assistidos pela equipe da Seção de Redes do Tribunal, a qual dará todo apoio e condições necessárias para realização das atividades;

3.1.5. O serviço de instalação e migração somente serão aceitos de forma provisória quando todas as funcionalidades estiverem com status operacionais;

3.1.6. O recebimento definitivo dos serviços de instalação e migração se dará no prazo de 10 (dez) dias após o recebimento provisório e se for constatada a estabilidade operacional da solução implantada;

3.2. Conforme descrito na Cláusula Segunda, caso a licitante oferte solução de fabricante diferente de Sonicwall deverá FORNECER SEM CUSTO AO TRIBUNAL os SERVIÇOS TREINAMENTO para qualificação técnica da equipe do TRE. Cujos serviços devem ser realizados obedecendo aos seguintes critérios:

3.2.1. TREINAMENTO OFICIAL

3.2.1.1. O curso a ser disponibilizado deverá pertencer ao catálogo de treinamentos oficiais do fabricante da solução ofertada;

3.2.1.2. Deverá abranger todos recursos técnicos da solução ofertada em nível avançado de configuração e gerenciamento dos firewalls;

3.2.1.3. Deverá disponibilizar material didático oficial para cada treinando;

3.2.1.4. Cada treinando que atingir as exigências do treinamento deverá receber Certificado;

3.2.1.5. O treinamento deverá ser presencial e poderá ser realizado na modalidade “in company” para 10 servidores designados pela Contratante. Caso o treinamento seja ministrado fora do ambiente do Tribunal, a LICITANTE deve prover sala de treinamento com todos os equipamentos necessários para a re-

alização do mesmo;

3.2.1.6. Para realização do treinamento deverá ser utilizado equipamentos iguais aos ofertados para fins de realização das baterias de exercícios e laboratórios, cujos equipamentos serão disponibilizados pela LICITANTE.

CLÁUSULA QUARTA - DO REGIME DE EXECUÇÃO

4.1 O objeto do presente instrumento será executado de forma indireta, sob o regime de empreitada por preço unitário, em conformidade com o disposto na Lei nº 8.666/1993.

CLÁUSULA QUINTA – DO PRAZO E CONDIÇÕES

5.1. A seguir estão registrados os prazos de entrega da Solução de Firewall Contratada:

5.1.2. A atualização dos equipamentos na modalidade de substituição deverão ser entregues em até 40 (quarenta) dias após a assinatura do Contrato ou do recebimento da Nota de Empenho.

5.1.3. Prazo de 10 (dez) dias após a entrega dos equipamentos substitutos para concluir a migração de todas as configurações existentes para os novos equipamentos, cujos serviços serão assistidos pela equipe de técnicos da Seção de Redes do Tribunal;

5.1.4. Caso a Contratada tenha ofertado solução de firewall de fabricante diferente da sonicwall, a mesma terá prazo de 20 (vinte) dias, após a entrega dos equipamentos substitutos, para realizar o treinamento oficial do fabricante para a equipe de 10 (dez) servidores da secretaria de TI do Tribunal, cujo treinamento deverá ser presencial e poderá ser na modalidade "in company", a ser realizado no ambiente de treinamento do Tribunal (Anexo I).

5.1.5. Os links ou outra forma de acesso dos usuários ao repositórios dos softwares de segurança integrantes da solução serão enviados mediante comunicação eletrônica para o endereço coinf@tre-al.jus.br e os serviços serão realizados na sede do Tribunal Regional Eleitoral de Alagoas, na Avenida Aristeu de Andrade, nº 377, Farol, Maceió, Alagoas.

5.1.6 Para realização dos serviços de instalação, configuração, migração e repasse de conhecimento a CONTRATADA deverá indicar profissional(is) capacitado(s) e qualificado(s) pelo fabricante da solução proposta, devidamente certificado para tal atividade.

5.2. LOCAL DE ENTREGA E QUANTITATIVOS

5.2.1. Os equipamentos deverão ser entregues na Seção de Almoxarifado e Patrimônio do TRE-AL, observadas as informações abaixo.

CNPJ	Responsável pelo recebimento	e-mail do responsável pelo recebimento	Contato do agendamento da entrega	Telefone	Horário	Endereço
06.015.041/0001-38	Seção de Almoxarifado	almoxarifado@tre-al.jus.br	Luciana ou Sérgio	(82) 3328-1947	8hs às 18hs de segunda a quinta-feira e entre 8hs e 16 hs às sextas-feiras	Av. Menino Marcelo, nº 7.200 D, Serraria Maceió/AL, CEP: 57046-000

5.3. A entrega ocorrerá mediante agendamento. O quadro acima apresenta o horário de funcionamento, no entanto poderá ser realizada entrega em período diverso, desde que haja anuência das partes.

5.4. Os equipamentos a serem entregues deverão atender rigorosamente a todas as especificações técnicas mínimas exigidas, inclusive modelos de peças e/ou componentes internos e externos ofertados na proposta vencedora.

5.5. No ato da entrega, a CONTRATADA emitirá à CONTRATANTE nota fiscal relacionando todos os Itens da Solução de Firewall entregues.

5.6. Findo o prazo estabelecido e comprovada a conformidade dos produtos com as especificações exigidas no edital e aquelas oferecidas pela CONTRATADA, a CONTRATANTE emitirá Termo de Recebimento Definitivo (TRD).

5.7. O prazo máximo para substituição do serviço que não atender às especificações será de 10 (dez) dias úteis, contados da data da notificação. Decorrido esse prazo e não havendo a devida substituição, serão aplicadas as penalidades legais cabíveis.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DAS PARTES

6.1. Compete ao CONTRATANTE:

a) Prestar informações, recomendações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;
b) promover o acompanhamento e a fiscalização dos produtos e serviços, sob os aspectos quantitativo e qualitativo;
c) designar servidor ou comissão de servidores para fiscalizar a execução do objeto contratual;
d) permitir que os funcionários da contratada, desde que devidamente

identificados, tenham acesso aos locais de entrega e instalação dos equipamentos;

e) recusar, a critério da fiscalização, qualquer serviço ou equipamentos fornecido ou executado fora das condições contratuais;

f) receber a solução contratada e acompanhar os serviços na forma descrita neste Termo de Referência;

g) efetuar o pagamento à CONTRATADA, segundo as condições estabelecidas neste Termo de Referência.

6.2. Compete à CONTRATADA:

a) Fornecer os produtos e serviços no prazo e demais condições estipuladas neste termo, no edital da licitação, proposta e no contrato;

b) seguir as instruções e observações efetuadas pelo gestor do contrato, bem como reparar, corrigir, reconstruir ou substituir às suas expensas, no todo ou em parte, os produtos ou serviços efetuados em que se verificarem vícios, defeitos ou incorreções;

c) executar, com observação dos prazos e exigências, as obrigações constantes do objeto deste Termo de Referência.

d) responsabilizar-se pelas despesas decorrentes da execução dos serviços objetos deste Termo de Referência, inclusive pelos encargos fiscais e comerciais resultantes da contratação.

e) garantir profissional capacitado e qualificado para realização dos serviços descritos no Termo de Referência, substituindo imediatamente se incapacitado para execução das atividades;

f) não transferir a outrem, no todo ou em parte, o objeto contratado, sem prévia anuência do CONTRATANTE;

g) manter durante a execução do contrato todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar à CONTRATANTE a superveniência de fato impeditivo da manutenção dessas condições;

h) responsabilizar-se por todo e qualquer dano que, por dolo ou culpa, os seus profissionais causarem a terceiros ou ao CONTRATANTE, devendo ser descontado do pagamento devido à CONTRATADA o valor correspondente aos prejuízos causados, conforme o caso;

i) Respeitar as normas de conduta e integridade do CONTRATANTE, primando sempre pelos princípios e valores descritos, responsabilizando-se pela orientação de seus profissionais para sua observância e integral respeito nas relações estabelecidas;

j) Respeitar as orientações e normas de controle de bens, de fluxo de pessoas nas dependências e de segurança da Informação da CONTRATANTE;

k) manter sigilo e a inviolabilidade das informações, sob pena de responsabilidade civil, penal e administrativa, de todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros que tomar conhecimento em razão da execução do contrato, devendo orientar seus empregados nesse sentido;

l) responsabilizar-se pela manutenção corretiva e suporte técnico em garantia e atualização dos softwares, pelo período descrito neste

Termo de Referência;

m) detalhar, documentar e repassar, conforme orientação e interesse do CONTRATANTE, todo o conhecimento técnico utilizado na execução dos serviços contratados; 9.3.14. promover o repasse total de conhecimento dos equipamentos instalados ao CONTRATANTE;

n) comunicar ao TRE, por escrito, quando verificar condições inadequadas de execução do objeto ou a iminência de fatos que possam prejudicar a sua execução e prestar os esclarecimentos que forem solicitados pelos fiscais;

o) prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CONTRATANTE, referentes a qualquer problema detectado ou ao andamento de atividades previstas;

p) Disponibilizar canal de atendimento para realização de requisições de execução de serviço ou resolução de dúvidas conforme descrito no Termo de Referência;

q) Comprovar a origem dos bens importados e a quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa, conforme art. 3º, III, do Decreto n. 7.174/2010;

r) Promover o repasse total de conhecimento da solução fornecida ao CONTRATANTE.

CLÁUSULA SÉTIMA - SERVIÇO DE INSTALAÇÃO/MIGRAÇÃO E TREINAMENTO OFICIAL

7.1. SERVIÇO DE INSTALAÇÃO/MIGRAÇÃO

7.1.1. A licitante vencedora deverá disponibilizar, no prazo constante deste Termo de Referência, técnicos devidamente certificados junto ao fabricante da solução ofertada para realizar todos os serviços de instalação/migração;

7.1.2. Os técnicos designados para essa missão deverão possuir experiências no processo de implantação de solução de firewall;

7.1.3. Toda a configuração existente em termos de enlace de redes, VPNs, rotas, objetos e regras de firewalls, etc., deverão ser migrados para nova solução ofertada;

7.1.4. Todos os serviços serão assistidos pela equipe da Seção de Redes do Tribunal, a qual dará todo apoio e condições necessárias para realização das atividades;

7.1.5. O serviço de instalação e migração somente serão aceitos de forma provisória quando todas as funcionalidades estiverem com status operacionais;

7.1.6. O recebimento definitivo dos serviços de instalação e migração se dará no prazo de 10 (dez) dias após o recebimento provisório e se for constatada a estabilidade operacional da solução implantada;

7.2. Conforme descrito no Item 7, caso a licitante oferte solução de fabricante diferente de Sonicwall deverá FORNECER SEM CUSTO AO TRIBUNAL os SERVIÇOS TREINAMENTO para qualificação técnica da equipe do TRE. Cujos serviços devem ser realizados obedecendo aos seguintes critérios

7.2.1. TREINAMENTO OFICIAL

7.2.1.1. O curso a ser disponibilizado deverá pertencer ao catálogo de

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

treinamentos oficiais do fabricante da solução ofertada;

7.2.1.2. Deverá abranger todos recursos técnicos da solução ofertada em nível avançado de configuração e gerenciamento dos firewalls;

7.2.1.3. Deverá disponibilizar material didático oficial para cada treinando;

7.2.1.4. Cada treinando que atingir as exigências do treinamento deverá receber Certificado;

7.2.1.5. O treinamento deverá ser presencial e poderá ser realizado na modalidade “in company” para 10 servidores designados pela Contratante. Caso o treinamento seja ministrado fora do ambiente do Tribunal, a LICITANTE deve prover sala de treinamento com todos os equipamentos necessários para a realização do mesmo;

7.2.1.6. Para realização do treinamento deverá ser utilizado equipamentos iguais aos ofertados para fins de realização das baterias de exercícios e laboratórios, cujos equipamentos serão disponibilizados pela LICITANTE.

CLÁUSULA OITAVA - DA GARANTIA TÉCNICA

8.1. A CONTRATADA deverá fornecer garantia técnica de 60 (sesenta) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação.

8.2. Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito durante este período, sem qualquer ônus adicional para o CONTRATANTE, obrigando-se a CONTRATADA a manter os equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam.

8.3. A garantia técnica compreenderá todas as funcionalidades da solução ofertada, tanto as descritas no Termo de Referência quanto as contempladas nos manuais e demais documentos técnicos, incluindo a atualização de versões de software.

8.4. Qualquer equipamento com hardware defeituoso, peças quebradas, com defeito ou desgastadas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 48 (quarenta e oito) horas a partir de notificação do CONTRATANTE.

8.5. A CONTRATADA deverá apresentar ao CONTRATANTE, antes do início da vigência do serviço de garantia técnica, todos os dados necessários para o registro de chamados técnicos em sua Central de Atendimento, tais como e-mail, números de telefone e fax etc.

8.6. A garantia técnica contemplará a manutenção dos equipamentos, requisitos de segurança integrantes, bem como os serviços de suporte na modalidade 8x5, para os equipamentos de pequeno porte (Sonicwall SOHO Wireless) ou equivalentes de outro fabricante.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

CLÁUSULA NONA - DO PREÇO E DO PAGAMENTO

9.1. O valor global do presente contrato é de R$ **108.750,00 (cento e oito mil e setecentos e cinquenta reais),** conforme proposta apresentada no certame licitatório.

9.2. O pagamento à CONTRATATA será efetuado em moeda corrente, no prazo de 15 (quinze) dias úteis após apresentação de Nota Fiscal/Fatura, em 1 (uma) via, devidamente atestada pela gestão do contrato.

9.3. Sobre as faturas incidirão os tributos legalmente instituídos e as multas que eventualmente vierem a ser aplicadas. Sendo a CONTRATATA isenta ou beneficiária de redução de alíquota de qualquer imposto, taxa ou de contribuição social ou ainda optante pelo SIMPLES, deverá apresentar junto com as faturas, cópia do comprovante respectivo.

9.4. Em caso de irregularidades na emissão dos documentos fiscais, o prazo de pagamento será contado a partir de sua reapresentação, devidamente regularizado. Nenhum pagamento será efetuado à CONTRATADA caso exista pendência quanto às condições de habilitação e qualificação exigidas na licitação.

9.5. O CONTRATANTE pode deduzir do montante a pagar os valores correspondentes a multas, ressarcimentos ou indenizações devidas pela CONTRATADA, nos termos deste contrato.

9.6. O Tribunal se reserva o direito de descontar do pagamento da contratada os eventuais débitos, inclusive os relacionados com multas, danos e prejuízos contra terceiros.

9.7. Para liquidação da despesa, a contratada deverá estar certidões de regularidade com a Previdência Social - CND/INSS e com o FGTS, em plena validade.

9.8. A CONTRATADA não poderá apresentar nota fiscal/fatura com CNPJ diverso do qualificado no preâmbulo deste Contrato.

8.9. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou á atualização monetária.

CLÁUSULA DEZ- DA VIGÊNCIA

10.1. O presente contrato terá vigência desde sua assinatura até o recebimento definitivo do objeto, ressalvado o período da garantia técnica, que será de 60 (sessenta) meses a contar do recebimento definitivo da fase de instalação.

CLÁUSULA ONZE - DO REAJUSTE

11.1. Os preços dos serviços poderão ser reajustados em atendimento a pedido expresso da CONTRATADA, conforme proposta de preços apresentada, tendo como limite máximo a variação do Índice Nacional de Preços ao Consumidor Amplo –

IPCA/IBGE dos últimos 12 (doze) meses, contados da data da apresentação da proposta de licitação ou do último reajuste.

CLÁUSULA DOZE – DA GARANTIA CONTRATUAL

12.1. A CONTRATADA apresentará, em até 10 (dez) dias úteis, contados da publicação deste instrumento na Imprensa Oficial, garantia de execução do contrato em uma das modalidades previstas em lei, em valor correspondente a 5% (cinco por cento) do valor do contrato, tendo como beneficiário o CONTRATANTE.

12.2. A garantia deverá ser prestada com vigência de 3 (três) meses após o término do período da garantia técnica.

12.3. A garantia apresentada deverá assegurar o pagamento de prejuízos advindos do não cumprimento do contrato, multas aplicadas à CONTRATADA e prejuízos diretos causados ao CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato.

12.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

12.5. Quando a garantia for apresentada na modalidade seguro-garantia, a apólice respectiva deverá ser expedida exclusivamente por qualquer das entidades controladas e fiscalizadas pela Superintendência de Seguros Privados (SUSEP). Deverá ser apresentado o número com que a apólice ou o endosso tenha sido registrado na SUSEP.

12.6. Quando a garantia for apresentada na modalidade fiança bancária, o instrumento respectivo deverá ser expedido exclusivamente por qualquer das entidades controladas e fiscalizadas pelo Banco Central do Brasil.

12.7. Quando a garantia for apresentada na modalidade fiança bancária, a instituição financeira fiadora deverá ser domiciliada ou possuir agência no Distrito Federal e demonstrar possuir bens suficientes à garantia integral da fiança prestada, conforme artigo 825 da Lei 10.406/2002. A carta de fiança deverá conter cláusula expressa de renúncia do fiador ao benefício de ordem previsto no artigo 827 da Lei n. 10.406/2002, conforme facultado pelo inciso I do artigo 828 do mesmo diploma legal, e ser registrada no Registro de Títulos e Documentos, conforme previsto nos artigos 128, 129 e 130 da Lei 6.015/73.

12.8. Alterado o valor do contrato, fica a CONTRATADA obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta cláusula, em até 10 (dez) dias úteis, contados da data de publicação do termo de aditamento na Imprensa Oficial.

12.9. Prorrogado o prazo de vigência do contrato, fica a CONTRATADA obrigada a renovar a garantia, no mesmo percentual e modalidades constantes desta cláusula, em até 10 (dez) dias úteis, contados da data de publicação do termo aditivo na Imprensa Oficial.

12.10. A garantia apresentada em desacordo com os requisitos e coberturas previstas no instrumento de contrato será devolvida à CONTRATADA, que disporá do prazo improrrogável de 10 (dez) dias úteis para a regularização da pendência.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

CLÁUSULA TREZE – DO ACEITE

13.1. Condições de aceite

13.1.1. A verificação técnica e o aceite definitivo da entrega da atualização da Solução de Firewall deverá ocorrer no prazo máximo de 10 (dez) dias úteis, contados do primeiro dia útil após a entrega de todos os produtos e serviços concluídos.

13.1.2. O aceite definitivo dos produtos e serviços será efetuado por comissão especialmente designada, que elaborarão relatório para fins de liberação do pagamento das Notas Fiscais/Faturas e para o início da contagem do prazo de vigência da Garantia, para manutenção dos Requisitos de Segurança, serviços de suporte técnico com substituição de equipamentos defeituosos.

CLÁUSULA CATORZE – DA PROPRIEDADE, SIGILO E RESTRIÇÕES

14.1. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA zelar por si e por seus sócios, empregados e subcontratados, pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados, conforme previsto no Decreto no 4.553, de 27 de dezembro de 2002.

14.2. A CONTRATADA responderá solidariamente com seus agentes empregados, prepostos, ou subcontratados, no caso de violação do compromisso de confidencialidade ora assumido.

14.3. O acesso à informação sigilosa será restrito ao funcionário alocado para a execução dos SERVIÇOS, não devendo este repassar a outros funcionários da CONTRATADA sem prévia autorização do CONTRATANTE.

14.4. A CONTRATADA deverá restituir imediatamente ao CONTRATANTE, quando do término do serviço ou quando for solicitada, qualquer informação deste. Em caso de perda de quaisquer informações, a CONTRATADA deverá notificar por escrito o CONTRATANTE, imediatamente.

14.5. A CONTRATADA será responsável pela assinatura do termo de ciência da declaração de sigilo e das normas de segurança, de conduta e integridade de todos os seus empregados diretamente envolvidos com a contratação.

14.6. A CONTRATADA obriga-se a manter sob sigilo absoluto os dados e/ou informações DA CONTRATANTE, ressalvados os casos cumprimento de exigência legal ou determinação judicial, casos em que deverá comunicar ao TRE-AL os exatos termos e abrangência respectiva da divulgação de dados, antecipadamente.

14.7. Qualquer exceção à obrigação de sigilo e confidencialidade aqui con-

tida depende de prévia e expressa autorização do Tribunal Regional Eleitoral de Alagoas.

CLÁUSULA QUINZE – DA FUNDAMENTAÇÃO LEGAL

15.1. O presente Contrato é celebrado mediante licitação na modalidade Pregão, na forma Eletrônica e sob o nº 28/2019, nos termos da Lei 10.520/2002, do Decreto 5.450, de 31 de maio de 2015, e, subsidiariamente, pela Lei 8.666, de 21 de junho de 1993.

CLÁUSULA DEZESSEIS – DO ACOMPANHAMENTO

16.1. A comissão especialmente designada pela Administração anotará em registro próprio todas as ocorrências relacionadas à gestão do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados (art. 67, §§ 1º e 2º da Lei 8.666/93) e notificando a autoridade superior, quando necessário, para as providências corretivas.

16.2. As relações mantidas entre o CONTRATANTE e a CONTRATADA serão intermediadas pela comissão responsável pela fiscalização do contrato.

16.3. À Fiscalização fica assegurado o direito de exigir o cumprimento fiel do contrato e impugnar todo e qualquer material ou serviços executados pela CONTRATADA, que não atendam às condições contratuais e a especificação técnica, cabendo à CONTRATADA refazer os serviços e/ou produtos rejeitados e arcar inteiramente com os custos decorrentes.

16.4. A existência e a atuação da fiscalização em nada restringem a responsabilidade única, integral e exclusiva da CONTRATADA, no que concerne à execução do objeto contratado.

CLÁUSULA DEZESSETE - DAS PENALIDADES

17.1. Pela inexecução total ou parcial do objeto contratado, a Contratada ficará sujeita às penalidades:

a) advertência por escrito à Contratada sobre o descumprimento de obrigações assumidas e a determinação da adoção das necessária as medidas de correção;
b) multa compensatória no percentual de até 15% (quinze por cento) calculada sobre o valor do contrato;
c) impedimento de licitar e contratar com a União e descredenciamento do SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste contrato e das demais penalidades legais;
d) declaração de inidoneidade para licitar ou contratar com a Administração Pública.

17.2 O atraso injustificado na entrega dos produtos ou serviços sujeitará a Contratada à multa de mora, sem prejuízo das demais sanções, inclusive a prevista no inciso IV, do art. 78, da Lei nº 8.666/93, que será aplicada na forma seguinte:

a) atraso de até 10 (dez) dias, multa diária de 0,4%, calculada sobre o valor do contrato;

b) atraso superior a 10 (dez) dias, multa diária de 0,7%, calculada sobre o valor do contrato, limitada a 10% (dez por cento), sem prejuízo da rescisão unilateral por parte da Administração.

17.3. O atraso injustificado na prestação de suporte técnico e atualização de versão sujeitará a Contratada à multa de mora, sem prejuízo das demais sanções, inclusive a prevista no inciso IV, do art. 78, da Lei nº 8.666/93, que será aplicada na forma seguinte:

a) multa de até 0,3% (três décimos por cento) sobre o valor do item afetado, por hora ou fração, em caso de atraso na resolução de chamados com severidade ALTA, limitado a 24 (vinte e quatro) horas;
b) multa de até 0,2% (dois décimos por cento) sobre o valor do item afetado, por dia ou fração, em caso de atraso na resolução de chamados com severidade MÉDIA, limitado a 30 (trinta) dias corridos;
c) multa de até 0,1% (um décimo por cento) sobre o valor do contrato, por dia ou fração, em caso de atraso na resolução de chamados com severidade BAIXA, limitado a 30 (trinta) dias corridos;
d) multa de até 1% (um por cento) sobre o valor total do contrato, por mês, caso o descumprimento dos prazos indicados nas alíneas acima exceda o limite estabelecido, para chamados de qualquer severidade, podendo ainda ser caracterizada a inexecução parcial do contrato;

17.4. Vencido o prazo ajustado sem o cumprimento da obrigação, total ou parcial, o Contratante oficiará à Contratada, comunicando-lhe a data-limite para fazê-lo. A entrega até a data-limite de que trata este item não isenta a Contratada da multa prevista nesta Cláusula;

17.5. O pedido de prorrogação extemporâneo ou não justificado na forma disposta será prontamente indeferido, sujeitando-se a Contratada às sanções previstas no instrumento contratual;

17.6. O valor da multa aplicada será retido dos pagamentos devidos pelo CONTRATANTE e, caso não sejam suficientes, a diferença será cobrada de acordo com a legislação em vigor;

17.7. A pena de multa poderá ser aplicada cumulativamente com as demais sanções previstas neste contrato;

17.8. As multas e outras sanções administrativas só poderão ser relevadas motivadamente por conveniência administrativa, mediante ato devidamente justificado, expedido pela autoridade competente;

17.9. As penalidades serão obrigatoriamente registradas no SICAF, e no caso de suspensão de licitar, a licitante será descredencia da por igual período, sem prejuízo das multas previstas no Edital e das demais cominações legais.

CLÁUSULA DEZOITO – SERVIÇO DE MANUTENÇÃO CORRETIVA EM GARANTIA

18.1. O prazo de manutenção corretiva em garantia é o mesmo da duração do contrato (incluídas as eventuais prorrogações), o qual será contado a partir da data da

emissão do Termo de aceite definitivo;

18.2. A manutenção em garantia poderá ser realizada pelo fabricante, porém, sendo responsabilidade subsidiária da CONTRATADA

18.3. Durante a vigência da manutenção em garantia, serão prestados os serviços de manutenção corretiva e direito de atualização de todos os softwares da solução, sem ônus para o CONTRATANTE;

18.4. Entende-se por manutenção corretiva em garantia a série de procedimentos destinados a recolocar os sistemas em seu perfeito estado de funcionamento, compreendendo, inclusive ajustes, reparos e atualização de versões necessárias, de acordo com a orientação do fabricante e normas técnicas específicas;

18.5. A manutenção corretiva deverá seguir as seguintes regras, referentes ao Chamado Técnico:

a) O atendimento técnico, referente à manutenção corretiva em garantia, será iniciado a partir da comunicação formal do evento, por parte dos técnicos autorizados, em português, através de telefone, e-mail ou outro meio informado, sem custo adicional de ligação para o CONTRATANTE;

b) A CONTRATADA deverá disponibilizar recursos para a abertura de solicitações de suporte técnico a qualquer momento, 24 horas por dia durante os 7 dias da semana;

c) Entende-se por “abertura do atendimento” a data e hora em que foi feito o acionamento da CONTRATADA, com o correspondente registro;

18.6. Os chamados deverão ser classificados conforme os níveis de severidade descritos a seguir:

a) Severidade Alta: problemas graves, que fazem com que a solução ou sistemas estejam indisponíveis para uso;
b) Severidade Média: problemas que afetam equipamentos ou componentes dos equipamentos, mas que não chegam a causar sua indisponibilidade, incluindo a troca de discos defeituosos; e
c) Severidade Baixa: problemas que não afetam o desempenho ou a disponibilidade dos sistemas, incluindo chamados para esclarecimento de dúvidas e atualização de versões;

18.7. Entende-se por “conclusão do atendimento” o pleno restabelecimento da funcionalidade e a execução de quaisquer procedimentos corretivos que se façam necessários;

18.8. Os chamados técnicos serão atendidos em até 8 (oito) horas úteis após a abertura do atendimento;

18.9. O tempo máximo para solução dos problemas varia de acordo com sua criticidade, conforme descrito a seguir:

a) Os problemas classificados como de Severidade Alta deverão ter a primeira resposta resolutiva para o caso em até 48 (quarenta e oito) horas, contadas a partir da abertura do chamado;
b) Os problemas classificados como de Severidade Média deverão ter a primeira resposta resolutiva para o caso em até 4 (quatro) dias úteis, contados a

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

partir da abertura do chamado;
c) Os problemas classificados como de Severidade Baixa deverão ter a primeira resposta resolutiva para o caso em até 10 (dez) dias úteis, contados a partir da abertura do chamado.

18.10. Todas as despesas que se fizerem necessárias para o atendimento correrão por conta da CONTRATADA;

18.11 A conclusão de um atendimento requer a concordância, por parte de um técnico designado pelo CONTRATANTE e será registrada;

18.12. A CONTRATADA deverá disponibilizar atendimento telefônico com pessoal habilitado a orientar a prestar suporte técnico;

18.13. A pedido a CONTRATADA apresentará um relatório de ocorrências, contendo data, hora de chamados, início e término do atendimento, as providências adotadas e toda e qualquer informação pertinente ao chamado;

18.14. Quanto trata-se de problema em unidade de armazenamento a unidade defeituosa deverá ser mantida com o CONTRATANTE para garantia do sigilo das informações;

18.15. Situações de exceção deverão ser avaliadas caso a caso, pela CONTRATADA, equipe Técnica do CONTRATANTE e pelo Gestor do Contrato, definindo os procedimentos mais adequados para o seu encaminhamento, levando em consideração a natureza da situação e eventuais consequências que possam surgir.

CLÁUSULA DEZENOVE - DA RESCISÃO

19.1. Constituem motivos para rescisão do presente contrato às hipóteses previstas no art. 77 e nos incisos I a XII e XVII do art. 78, da Lei 8.666/93, e alterações posteriores.

19.2. Os casos de rescisão contratual pelos motivos previstos nesta cláusula serão formalmente motivados em processo.

19.3. A rescisão contratual, precedida da devida autorização do CONTRATANTE, na forma escrita e fundamentada, poderá ser:

a) Formalizada através de ato unilateral do CONTRATANTE, na ocorrência dos motivos previstos nesta cláusula;
b) Amigável, por acordo das partes, desde que haja conveniência para o CONTRATANTE, mediante termo cabível;
c) Judicial, nos termos da legislação.

CLÁUSULA VINTE - DA DOTAÇÃO ORÇAMENTÁRIA

20.1. A despesa decorrente do presente Contrato correrá à conta do Programa de Trabalho: 02.122.0570.20GP.0017 – Julgamento de Causas e Gestão Administrativa da Justiça Eleitoral e Elemento de Despesa: 4.4.9.0.52.37 - Equipamentos e Material Permanente/Equipamentos de TIC – Ativos de Rede.

PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS

CLÁUSULA VINTE E UM – DA PUBLICAÇÃO

21.1. O presente Contrato será publicado em extrato no D.O.U., consoante termos do artigo 61, Parágrafo Único, da Lei nº. 8.666/1993, às expensas do Contratante.

CLÁUSULA VINTE E DOIS - DO FORO

22.1. Fica eleito o foro da Justiça Federal, Seção Judiciária do Estado do Alagoas em Maceió, com renúncia expressa a outros, por mais privilegiados que sejam, para dirimir quaisquer questões fundadas neste Contrato.

E por estarem assim de pleno acordo, firmam as partes o presente instrumento.

Maceió/AL, 16 de junho de 2020.

Pelo TRE/AL:

OTAVIO LEAO PRAXEDES:3092M145

Digitally signed by OTAVIO LEAO PRAXEDES:3092M145
DN: cn=OTAVIO LEAO PRAXEDES:3092M145, c=BR, o=ICP-Brasil, ou=MAGISTRADO, email=otaviopraxedes@tre-al.jus.br
Date: 2020.06.19 11:08:12 -03'00'

Desembargador Otávio Leão Praxedes
Vice-Presidente no exercício da Presidência do TRE/AL

Pela CONTRATADA:

Sr. José Jacob Nácul

JOSE JACOB NACUL:03723664814

Assinado de forma digital por JOSE JACOB NACUL:03723664814
Dados: 2020.06.18 08:37:26 -03'00'

PROPOSTA 027/2020-GOV

COTAÇÃO DE PREÇO

Ao

Tribunal Regional Eleitoral do Piauí – TER-PI

Aos Cuidados do Sr. Carlos Alberto Ribeiro do Nascimento Jr.

Seção de Infraestrutura - CODIN – STI

e-mail: carlos.nascimento@tre-pi.jus.br

Fone: +55 86 2107-9756 / 9778

Objeto: Atualização de solução **SONICWALL** de acordo com a especificação técnica contida no anexo 01 – Especificação Técnica Mínimas dessa proposta técnica e comercial.

Part Number	Descrição	Valor em reais - UN	Quantidade	Valor Total
01-SSC-1939	SONICWALL NSA 5650 APPLIANCE	R$ 176.107,25	1	R$ 176.107,25
01-SSC-3217	SONICWALL NSA 5650 HIGH AVAILABILITY	R$ 123.331,13	1	R$ 123.331,13
01-SSC-3678	ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 5650 5YR	R$ 325.169,32	1	R$ 325.169,32
02-SSC-1865	SONICWALL SOHO 250 WIRELESS-N INTL	R$ 7.608,09	1	R$ 7.608,09
02-SSC-1724	24X7 SUPPORT FOR SOHO 250 SERIES 5YR	R$ 3.836,50	1	R$ 3.836,50
TOTAL				**R$ 636.052,29**

- ✓ Valor por extenso: R$ 636.052,29 (Seiscentos e trinta e seis mil, cinquenta e dois reais e vinte e nove centavos);
- ✓ Validade da proposta: 60 (sessenta) dias;
- ✓ Prazo de entrega da solução é de 30 (trinta) dias.

Dados da Empresa

- ✓ Nome/ Empresa: Disruptec Brasil Ltda;
- ✓ CNPJ: 11.038.368/0001-65;
- ✓ Endereço: CLN 7 Bloco D Lote 4 Loja 7 – Brasília – DF;

Telefone/fax/e-mail: 061 3081-6217.

Brasília – DF, 31 de agosto de 2020

ELMIRO CESAR BARBOSA NETO:03484045655
Assinado de forma digital por ELMIRO CESAR BARBOSA NETO:03484045655 Dados: 2020.08.31 17:19:04 -03'00'

Elmiro Cesar Barbosa Neto
Comercial
DISRUPTEC BRASIL
contato@disruptec.com.br

teltec SOLUTIONS

Cliente: Tribunal Regional Eleitoral do Piauí

TRE PI

Proposta: Proposta Segurança

V2.0

Com 28 anos de mercado, a Teltec Solutions possui sua sede em Florianópolis e filiais em Brasília e São Paulo. Com experiência no atendimento de mais de **700 cliente**s e atuação em **todo o território nacional,** propomos soluções para os mais diferentes cenários, encontrando o melhor custo-benefício para entregar as melhores soluções do mercado sempre de acordo com os desafios e necessidades de cada cliente.

28 ANOS DE MERCADO

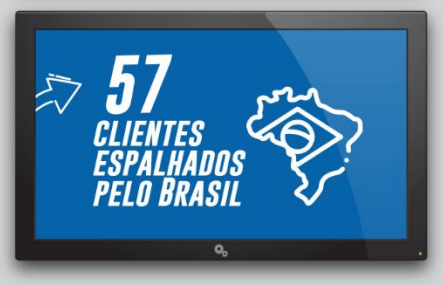
287 CERTIFICAÇÕES ATIVAS

120.000+ HORAS DE PROJETO

700+ CLIENTES

TODO TERRITÓRIO NACIONAL

Monitoramos Mais de



NOC TELTEC

- 24 HORAS POR DIA
- 7 DIAS POR SEMANA

Somos especialistas nos principais Players do Mercado

Cisco · Microsoft · aws · paloalto
vmware · NetApp · CITRIX · IBM
milestone · f5 · Google · AXIS COMMUNICATIONS

SOLUÇÕES

- Firewall e Segurança de Rede
- Gerenciamento de Projetos e Serviços de Instalação
- Minecraft For Education
- Monitoramento IP para Segurança Física
- Software de Gerenciamento
- Hiperconvergência
- Gerenciamento de Infraestrutura - NOC 24x7
- Armazenamento de Dados
- Telefonia IP e Videoconferência
- Redes (Switches)
- Roteadores
- Virtualização
- SD-WAN
- Servidores Onpremisse e Cloud
- Backup On-premises e Cloud
- Cloud Computing
- Visibilidade de Aplicações e Negócios
- Wi-Fi

Cisco Gold Partner · Citrix Gold Solution Advisor · paloalto Platinum Partner · aws Advanced Consulting Partner · NetApp Gold Partner · AXIS Gold Partner · Microsoft Gold Partner

Florianópolis, 02 de setembro de 2020.

Referência: Proposta Segurança

Prezados

Agradecemos a oportunidade de nos apresentarmos e o interesse nas soluções Teltec Solutions.

Em conformidade com as tratativas ocorridas, encaminhamos proposta comercial para fornecimento de equipamentos Cisco.

Sendo o que se apresenta para o momento, nos colocamos a sua disposição para o esclarecimento de quaisquer dúvidas.

Ana Carolina Silva
Executiva de Vendas

Rodrigo Salvo
Analista de Soluões

1. **Condições comerciais:**

Item	DESCRIÇÃO DO MODELO	Qtd	Valor Unit	Valor Total
FASE 1				
1	Cisco Firepower 1150 NGFW Appliance, 1U TELTEC SUPORTE8X5XNBD Cisco Firepower 1150 NGFW Appliance, 1U Cisco FPR1150 Threat Defense Threat, Malware and URL 3Y Subs 10GBASE-CU SFP+ Cable 5 Meter	2	R$220.000,00	R$440.000,00
2	Cisco Firepower Management Center,(VMWare) for 2 devices TELTEC SUPORTEUPGRADES-Cisco FireSIGHT Management CenterVMWare ISE Passive Identity Connector Virtual Machine 3000 sessions TELTEC SUPORTEUPGRADES Identity Services Engine Passive Identit Cisco AnyConnect Plus License, 3YR, 25-99 Users	1	R$17.200,00	R$17.200,00
				Total R$ 457.200,00
FASE 2				
3	Cisco Firepower 1010 NGFW Appliance, Desktop TELTEC SUPORTE8X5XNBD Cisco Firepower 1010 NGFW Appliance, Des	69	R$ 6.800,00	R$ 469.200,00
				Total R$ 469.200,00
4	Cisco Firepower Management Center 2600 Chassis TELTEC SUPORTE8X5XNBD Cisco Firepower Management Center 2600 C	1	R$ 485.000,00	R$ 485.000,00
				Total R$ 485.000,00

2. Condições gerais da proposta comercial:

Nos preços acima cotados estão inclusos todos os impostos, taxas, frete e demais despesas que venham a incidir sobre o valor da proposta.

Os valores cotados em dólares americanos serão convertidos de acordo com a taxa PTAX do dia anterior ao faturamento/emissão da nota fiscal.

Prazo de entrega/instalação: Os produtos/serviços serão entregues em até 60 dias, contados do recebimento do pedido de compra/proposta assinada. A instalação ocorrerá em até 30 dias, contados a partir da entrega dos produtos.

Validade da proposta: Esta proposta comercial é válida por 45 dias, contatos da sua apresentação.

Confidencialidade: A TELTEC Solutions garante a confidencialidade das informações, dados, senhas e documentos que venha a ter acesso em razão da execução dos produtos/serviços adquiridos.

Os produtos/serviços serão faturados por:
TELTEC Solutions LTDA
CNPJ: 04.892.991/0001-15
Endereço: Rua Miguel Daux, 100, bairro Coqueiros, Florianópolis / SC, CEP 88.080-220.

Permanecemos à disposição

Ana Carolina Silva
Teltec Solutions
48 30313450