CONTRATO PARA FORNECIMENTO DE EQUIPAMENTOS DE REDE DE COMPUTADORES, QUE ENTRE SI CELEBRAM A UNIÃO, POR INTERMÉDIO DO TRIBUNAL REGIONAL ELEITORAL DA BAHIA, E A EMPRESA NOVA COMÉRCIO TECNOLOGIAS DE INFORMÁTICA EIRELI.

CONTRATO Nº 44/2019

A UNIÃO, por intermédio do **TRIBUNAL REGIONAL ELEITORAL DA BAHIA,** com sede na 1ª Avenida do Centro Administrativo da Bahia, n.º 150, Salvador - BA, inscrito no CNPJ/MF sob o n.º 05.967.350/0001-45, doravante denominado **Contratante,** neste ato representado por seu Diretor-Geral, Raimundo de Campos Vieira, no uso da competência que lhe é atribuída pelo Regulamento Interno da Secretaria do TRE-BA, e a empresa **NOVA COMÉRCIO TECNOLOGIAS DE INFORMÁTICA EIRELI**, inscrita no CNPJ/MF sob o n.º 05.847.161/0001-39, com sede na SRTVS, Quadra 701. Bl. O, Lote 04, Ed. Multiempresarial, sala 385, Asa Sul, Brasília- DF, telefone n.º (61) 3032-6602, *e-mail* administrador@grupoinova.com.br, doravante denominada **Contratada,** representada neste ato pelo Sr. José Jacob Nácul, portador da Carteira de Identidade n.º 4015908439 – SSP/RS, inscrito no CPF/MF sob n.º 037.236.648-14, resolvem celebrar o presente **CONTRATO PARA FORNECIMENTO DE EQUIPAMENTOS DE REDE DE COMPUTADORES,** albergado na Lei n.º 8.666/93 e alterações posteriores, resultante do **Pregão n.º 61/2018**, consoante Processos Administrativos Digitais (PAD) n.º 4.387/2018 e 12.346/2019.

CLÁUSULA PRIMEIRA – *DO OBJETO*

1. O objeto do presente contrato é o fornecimento de equipamentos de Rede de Computadores**,** conforme as condições estabelecidas no Edital de Pregão n.º **61/2018** e na proposta firmada pela Contratada, que passam a integrar este instrumento, independentemente de transcrição.

CLÁUSULA SEGUNDA - *DO VALOR CONTRATAUAL*

ITEM	DESCRIÇÃO	QUANT.	Valor unitário (R$)	Valor total (R$)
7	Licença para Solução Unificada de Segurança da Sede.	01 unidade	70.000,00	70.000,00

1. O valor total do presente contrato é de R$ 70.000,00 (setenta mil reais).

1.1. O valor acima referido inclui todos os custos diretos e indiretos, bem como deveres, obrigações e encargos de qualquer natureza, não sendo devido à Contratada qualquer outro pagamento resultante da execução deste ajuste.

CLÁUSULA TERCEIRA – *DA DOTAÇÃO ORÇAMENTÁRIA*

1. A despesa correrá à conta do elemento 3.33.90.40.06 "Locação de Software", vinculado à Ação 02.122.0570.20GP.0029 – "Julgamento de Causas e Gestão Administrativa na Justiça Eleitoral – no Estado da Bahia"", do Programa "Gestão do Processo Eleitoral".

2. Para a cobertura das despesas, foi emitida a Nota de Empenho n.º 2019NE002169, em 04 de setembro de 2019.

CLÁUSULA QUARTA – *DA ENTREGA, DO RECEBIMENTO E DA GARATIA DE ADEQUAÇÃO DO PRODUTO*

1. A entrega e o recebimento do objeto contratado serão efetuados em conformidade com o disposto no Termo de Referência, Anexo I, do Edital, que passa a integrar este instrumento contratual.

2. No momento da entrega, será exigida a comprovação da origem dos bens importados e da quitação dos tributos de importação a eles referentes, sob pena de rescisão contratual e multa.

3. A Contratada deverá oferecer garantia, pelo prazo constante na descrição de cada item, contra qualquer vício de fabricação e montagem/instalação, a partir do recebimento definitivo.

4. A Contratada deverá assegurar o cumprimento da garantia/assistência técnica **por parte do fabricante**, durante o respectivo período de vigência, sem ônus adicionais para o Contratante; caso não sejam prestadas na forma contemplada pelo Termo de Referência (Anexo deste Contrato.), fica a Contratada sujeita às penalidades insculpidas no item 8 do aludido documento.

5. A Contratada obriga-se a efetuar o atendimento aos chamados para prestação de assistência técnica decorrente da garantia, na forma e prazos previstos no Tópico 5 do Termo de Referência (Anexo deste Contrato.).

CLÁUSULA QUINTA – *DAS OBRIGAÇÕES DA CONTRATANTE*

1. A Contratante obriga-se a:

a) acompanhar e fiscalizar a execução do ajuste, anotando em registro próprio as ocorrências acaso verificadas, determinando o que for necessário à regularização das faltas ou defeitos observados;

b) prestar esclarecimentos que venham a ser solicitados pela Contratada;

c) efetuar os pagamentos nas condições e nos prazos constantes dos instrumentos convocatório e

contratual;

d) zelar para que, durante a vigência do Contrato, a Contratada cumpra as obrigações assumidas, bem como sejam mantidas as condições de habilitação e qualificação exigidas no processo licitatório;

e) determinar a reparação, a correção, a remoção, a reconstrução ou a substituição do objeto contratado que apresentar vícios ou incorreções resultantes da execução ou de materiais empregados ou do seu uso correto, que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor.

CLÁUSULA SEXTA – *DAS OBRIGAÇÕES DA CONTRATADA*

1. São obrigações da Contratada, além daquelas explícita ou implicitamente contidas no presente Contrato, no Termo de Referência e na legislação vigente:

a) entregar os bens no prazo, nas especificações e na quantidade constantes neste contrato, assim como com as características descritas na proposta;

b) atender às solicitações da Contratante nos prazos estabelecidos neste instrumento;

c) não fornecer quantidade ou modelo diverso do solicitado;

d) substituir os produtos danificados em razão de transporte, descarga ou outra situação que não possa ser imputada à Administração;

e) responder pelos encargos previdenciários, trabalhistas, fiscais e comerciais resultantes da execução deste Contrato;

f) responder por quaisquer danos pessoais ou materiais causados por seus empregados à Administração e/ou a terceiros na execução deste Contrato;

g) manter, durante a execução do ajuste, todas as condições de habilitação exigidas para a contratação;

h) reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto contratado que apresentar vícios ou incorreções resultantes da execução ou de materiais empregados ou do seu uso correto, que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor;

i) não subcontratar, ceder ou transferir, no todo ou em parte, o objeto deste contrato;

j) conferir garantia de adequação dos produtos (qualidade, segurança, durabilidade e desempenho), em conformidade com as condições estabelecidas no Termo de Referência, Anexo deste Contrato.

CLÁUSULA SÉTIMA – *DO PAGAMENTO*

1. O pagamento será efetuado na forma e prazos estabelecidos no Termo de Referência, Anexo deste

Contrato.

2. Por ocasião do pagamento, deverá ser verificada a regularidade da Contratada perante a Fazenda Nacional (Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União), o Fundo de Garantia do Tempo de Serviço (Certificado de Regularidade do FGTS – CRF), a Justiça Trabalhista (Certidão Negativa de Débitos Trabalhistas - CNDT) e a Fazenda Estadual/Distrital (Certidão de Quitação de Tributos Estaduais/Distritais ou Certidão que comprove a regularidade com o ICMS, emitida pelo órgão competente).

3. A Contratada indicará na nota fiscal/fatura o nome do Banco e os números da agência e da conta corrente para efetivação do pagamento.

4. Observados os princípios do contraditório e da ampla defesa, a Contratante poderá deduzir os valores correspondentes a multas, ressarcimentos ou indenizações, devidos pela Contratada, do montante a ser-lhe pago.

5. No caso de atraso de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, serão devidos pela Contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

6. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

CLÁUSULA OITAVA – *DA VIGÊNCIA*

1. A vigência do contrato será de 16 meses, a contar da data de sua assinatura.

1.1. O pagamento será realizado de uma única vez, após o recebimento definitivo do bem, na forma e nos prazos previstos no Termo de Referência (Anexo a este Contrato).

CLÁUSULA NONA – DAS SANÇÕES PELO DESCUMPRIMENTO DAS OBRIGAÇÕES CONTRATUAIS

1. De acordo com o disposto no art. 7º da Lei nº 10.520/2002, ficará IMPEDIDA DE LICITAR E DE CONTRATAR com a União e será descredenciada do SICAF e dos sistemas de cadastramento de fornecedores do TRE-BA, PELO PRAZO DE ATÉ 5 (CINCO) ANOS, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantidos o contraditório e a ampla defesa, a licitante que:

a) não mantiver a proposta, injustificadamente;

b) comportar-se de modo inidôneo;

c) fizer declaração falsa;

d) cometer fraude fiscal;

e) falhar ou fraudar na execução do contrato;

f) não encaminhar documentação exigida no certame ou entregar documentação falsa;

g) não fornecer o objeto licitado;

h) retardar a entrega do objeto licitado;

i) fornecer material que não atenda à especificação exigida no edital.

2. Para os fins da alínea "b", reputar-se-ão inidôneos atos como os descritos nos arts. 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93.

3. A recusa injustificada do adjudicatário em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas.

4. Qualquer penalidade somente poderá ser aplicada mediante processo administrativo, no qual se assegurem a prévia defesa e o contraditório, consoante rito estabelecido no art. 87, § 2º da Lei 8.666/93, aplicando-se, subsidiariamente, a Lei nº 9.784/99 e a Portaria nº 455/2016, da Presidência do TRE-BA.

5. Pelo inadimplemento total ou parcial das obrigações assumidas, a Contratada estará sujeita à multa prevista no Termo de Referência, Anexo deste Contrato.

6. A Contratante poderá reter dos pagamentos devidos à Contratada, como medida cautelar, independentemente de sua manifestação prévia, valor relativo a eventual multa a ser aplicada em razão de inadimplemento contratual, com base no artigo 45 da Lei nº 9.784/99 e no artigo 7º, parágrafo único, da Portaria nº 455/2016, da Presidência do TRE/BA.

7. O valor da multa aplicada será descontado dos pagamentos eventualmente devidos à licitante vencedora ou da garantia prestada, quando houver, ou ainda, quando for o caso, cobrado judicialmente.

8. Aplicada a penalidade de multa, após regular processo administrativo, observado o disposto nos **itens 6 e 7, desta Cláusula**, será a Contratada, se for o caso, intimada para efetuar o recolhimento do seu valor por meio de Guia de Recolhimento da União – GRU, no prazo de 30 dias, contados da intimação.

9. As situações mencionadas nos incisos I a XII, XVII e XVIII do art. 78 da Lei 8.666/93 podem ensejar, a critério da Administração, a rescisão unilateral do contrato.

10. Os recursos contra a aplicação de sanções em decorrência de inadimplemento contratual serão dirigidos à Presidência do TRE-BA, sendo interpostos na forma e nos prazos estabelecidos no art.109 da Lei 8.666/93.

CLÁUSULA DÉCIMA– *DA ALTERAÇÃO DO CONTRATO*

1. Este contrato poderá ser alterado nos casos previstos no art. 65 da Lei 8.666/93, desde que haja interesse da Contratante, com a apresentação das devidas justificativas.

CLÁUSULA DÉCIMA PRIMEIRA – *DA RESCISÃO CONTRATUAL*

1. A inexecução total ou parcial do Contrato enseja a sua rescisão, conforme disposto nos artigos 77 a 80 da Lei 8.666/93, sem prejuízo da aplicação das penalidades aqui estabelecidas.

2. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA SEGUNDA– *DA PUBLICAÇÃO*

1. O presente contrato será publicado, em extrato, no Diário Oficial da União, conforme prescreve o art. 61, parágrafo único, da Lei 8.666/93.

CLÁUSULA DÉCIMA TERCEIRA – *DO FUNDAMENTO LEGAL*

1. O presente Contrato é celebrado com fulcro nas normas insertas na Lei 8.666/93 e suas alterações, tendo por base as condições estabelecidas no Pregão nº 61/2018 e os termos da proposta apresentada pela Contratada.

CLÁUSULA DÉCIMA QUARTA – *DO FORO*

1. Fica eleito o foro da Seção Judiciária da Justiça Federal de Salvador, capital do Estado da Bahia, para dirimir qualquer dúvida oriunda da execução deste contrato.

E, por estarem justas e contratadas, assinam as partes o presente instrumento, em 02 (duas) vias de igual teor e forma, para que produza seus jurídicos e legais efeitos.

Salvador, _____ de _____ de 2019.

RAIMUNDO DE CAMPOS VIEIRA:13353578587
Assinado de forma digital por RAIMUNDO DE CAMPOS VIEIRA:13353578587
Dados: 2019.09.13 08:05:21 -03'00'

JOSE JACOB NACUL:03723664814
Assinado de forma digital por JOSE JACOB NACUL:03723664814
Dados: 2019.09.11 14:23:11 -03'00'

Raimundo de Campos Vieira
Diretor-Geral do TRE-BA

José Jacob Nácul
CPF nº 037.236.648-14
NOVA COMÉRCIO TECNOLOGIAS DE INFORMÁTICA EIRELI

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Registro de Preços para Eventual Aquisição de Equipamentos de Rede de Computadores, conforme especificações detalhadas constantes no Anexo A deste Termo de Referência.

2. JUSTIFICATIVA

2.1. Troca de equipamentos críticos em fim de vida útil ou defeituosos, bem como a ampliação do quantitativo existente por conta de novas necessidades, conforme detalhado nos estudos preliminares. Fazem parte dessa iniciativa: comutadores centrais, comutadores de borda, comutadores de cartório, *transceivers* para comutadores, soluções integradas de segurança de pequeno porte (para cartórios) e de grande porte (para a Sede), incluindo licenças de software de gerenciamento integrado para esse tipo de equipamento.

A modalidade de registro de preços é a que mais se adequa às aquisições, visto que todos os itens aqui estão sujeitos a um grau de indeterminação quanto ao quantitativo da eventual aquisição ou quanto ao momento da sua eventual aquisição, considerando-se que ou estão associados a demandas em quantidades variáveis, como postos de atendimento biométrico, ou estão dependentes de conclusão de fases da reforma do cabeamento de rede predial, conduzida através do Processo Nº: 013572/2017, traduzindo-se na prática em condições de entregas parceladas ou quantitativo não definido previamente, em consonância ao previsto no art. 3º do Decreto 7892/2013, incisos II e IV:

> *II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;*
>
> *IV – quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.*

Para todos os itens a modalidade de licitação indicada é o **pregão eletrônico**. Por questões de compatibilidade detalhadas a seguir, houve indicação de marca e modelo para todos os itens, à exceção do item 5, para os quais foram apresentados modelos referenciais de variadas marcas. Os itens 1, 2, 3 e 4 devem ser agrupados em um lote (LOTE 1) pela necessidade de serem de um mesmo fabricante. Especificamente, por se tratarem de equipamentos críticos e muito complexos, que definem centenas de protocolos de rede e funcionalidades que precisam coexistir em perfeita compatibilidade e por se tratar de equipamentos que compõem o cerne da rede de computadores da Justiça Eleitoral da Bahia, não podem existir vazios nos limites de responsabilidade entre múltiplos fabricantes ou revendas associados a esses equipamentos. Assim, além da necessidade de manter inteira **compatibilidade** entre os equipamentos, há a necessidade de que eles sejam instalados pelo mesma empresa que os fornecer, nas quantidades exatas que são necessárias para que formem um conjunto funcional, de modo a assegurar o pleno funcionamento ao final do processo de instalação. O item 6 servirá para conexão primária junto ao Tribunal Superior Eleitoral e há necessidade de compatibilidade total do equipamento adotado aqui com o equipamento

adotado naquele Tribunal Superior, como parte da padronização adotada pelo próprio TSE. Por fim, os itens 7 e 8 são licenças de software produzidas pelo fabricante dos equipamentos de modelos específicos indicados, que já foram adquiridos pelo TRE-BA, e que habilitam funcionalidades nesses equipamentos. Não havendo portanto outros tipos compatíveis de outros fabricantes. **Por isso, para o LOTE 1 e itens 6, 7 e 8, constam as especificações técnicas detalhadas como referência, mas foram indicados marca e modelos específicos**. Para o item 5 constam as especificações gerais com a indicação dos modelos de referência. Ainda com relação ao item 5, cabe ressaltar a impossibilidade de aplicação especificamente do inciso III do artigo 48 da Lei Complementar nº 123/2006 e do inciso IV do artigo 2º do Decreto nº 8.538/2015, devido à necessidade de padronização desses equipamentos em todos os cartórios eleitorais por motivo da implementação da gerência remota centralizada.

O Prazo Contratual para os contratos que envolvam exclusivamente os itens 7 e 8 (contratos com garantia de 12 meses) deverá ser de 16 meses após a assinatura. Para contratos que envolvam os itens do Lote 1 (itens 1 a 4) e o item 6, o prazo deverá ser de 40 meses após a assinatura. Para o Item 5, o termo de contrato será substituído por Nota de Empenho.

A modalidade de licitação sugerida para este registro de preços é o **pregão eletrônico**, com **preço por lote para os itens 1 a 4**, e, para os demais, **preço por item**.

2.1.1. Relação Demanda Prevista e Quantidade a Ser Contratada.

LOTE	ITEM	DESCRIÇÃO	QUANTIDADE
L O T E 1	1	Comutador Central. As especificações detalhadas constam no Anexo A deste Termo de Referência.	02 unidades
	2	Comutador de Borda. As especificações detalhadas constam no Anexo A deste Termo de Referência.	55 unidades
	3	Transceiver 10GBASE-LR. As especificações detalhadas constam no Anexo A deste Termo de Referência.	120 unidades
	4	Transceiver 10GBASE-SR. As especificações detalhadas constam no Anexo A deste Termo de Referência.	120 unidades
ITEM		DESCRIÇÃO	QUANTIDADE
5		Comutador para Cartório As especificações detalhadas constam no Anexo A deste Termo de Referência.	200 unidades

6	Solução Unificada de Segurança. As especificações detalhadas constam no Anexo A deste Termo de Referência.	02 unidades
7	Licença para Solução Unificada de Segurança da Sede. As especificações detalhadas constam no Anexo A deste Termo de Referência.	01 unidade
8	Licença para Solução Unificada para Cartório. As especificações detalhadas constam no Anexo A deste Termo de Referência.	300 unidades

3. LOCAL E PRAZO DE ENTREGA

3.1. A Contratada deverá entregar o material na SEGEP, localizada no Edifício-Sede do Tribunal Regional Eleitoral da Bahia (TRE-BA), sito na 1ª Avenida do Centro Administrativo da Bahia, nº 150, Salvador – Bahia.

3.2. Horários de entrega: 13h às 18h, de segunda à quinta-feira, e 08h às 12h, às sextas-feiras.

3.3. A Contratada deverá, obrigatoriamente, consultar a SEGEP, através dos telefones (71) 3373-7077 ou (71) 3373-7357), ou através do e-mail segep@tre-ba.jus.br, para fazer o agendamento da entrega.

3.4. O prazo para a entrega do material será de **quarenta dias úteis**, contados do recebimento pela contratada do "Pedido de Fornecimento", que será emitido pela fiscalização do contrato, durante a vigência do registro de preços a ser firmado.

3.5. Correrão por conta da contratada quaisquer providências relativas à descarga do material, incluindo-se aí a necessária mão de obra.

3.6. Em caso de paralisação das atividades dos setores responsáveis pelo recebimento dos bens durante o Recesso Forense (entre 20 de dezembro e 6 de janeiro do ano subsequente), haverá a suspensão dos prazos de entrega em favor da Contratada. Neste caso, a empresa será previamente notificada pela Fiscalização do Contrato.

4. RECEBIMENTO

4.1. O recebimento ocorrerá em duas etapas:

a) **Recebimento provisório**: o material será recebido provisoriamente no momento da entrega, para efeito de posterior verificação de sua conformidade com as especificações constantes do Edital e da proposta, ficando, nesta ocasião, suspensa a fluência do prazo de entrega inicialmente fixado.

b) **Recebimento definitivo**: no prazo de **5 dias úteis** dias após o recebimento provisório, a Fiscalização do Contrato avaliará as características do material que, estando em conformidade com as especificações exigidas, será recebido definitivamente.

4.2. A Contratada garantirá a qualidade do material fornecido, obrigando-se a substituir aquele que apresentar vícios ou incorreções resultantes da fabricação ou de sua correta utilização, que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor.

4.3. Em caso de irregularidades apuradas no momento da entrega, o material poderá ser recusado de pronto, mediante termo correspondente, ficando dispensado o recebimento provisório, e fazendo-se disso imediata comunicação escrita ao fornecedor.

4.4. Se após o recebimento provisório, constatar-se que o fornecimento foi efetuado em desacordo com o pactuado ou foi entregue quantitativo inferior ao solicitado, a Fiscalização do Contrato notificará por escrito a Contratada para substituir, às suas expensas, o material recusado ou complementar o material faltante, no prazo que lhe restar daquele indicado para entrega.

4.5. Se a Contratada não substituir ou complementar o material entregue em desconformidade com as condições exigidas no edital, o fiscal do contrato glosará a nota fiscal, no valor do material não entregue ou recusado, e a encaminhará para pagamento, acompanhada de relatório circunstanciado, informando, ainda, o valor a ser retido cautelarmente, para fazer face a eventual aplicação de multa.

4.6. Caso a Contratada não retire, no prazo de 90 dias, a contar do recebimento da notificação, o material recusado, ficará caracterizado o seu abandono, nos termos do disposto no artigo 1.275, Inciso III, do Código Civil, podendo a Contratante incorporá-lo ao seu patrimônio, encaminhá-lo a outros órgãos da Administração Pública ou, ainda, a entidades filantrópicas sem fins lucrativos, reconhecidas como de utilidade pública federal, e a Organizações da Sociedade Civil de Interesse Público.

4.7. A Contratada fará constar da nota fiscal os valores unitários e respectivos valores totais em conformidade com o constante da correspondente nota de empenho/contrato, atentando-se para as inexatidões que poderão decorrer de eventuais arredondamentos.

4.8. Consoante o disposto no artigo 32 da Lei n° 12.305/2010, as embalagens dos materiais devem ser fabricadas com materiais que propiciem a reutilização ou a reciclagem, devendo-se assegurar que sejam restritas em volume e peso às dimensões requeridas à proteção do conteúdo e à comercialização do produto, projetadas de forma a serem reutilizadas de maneira tecnicamente viável e compatível com as exigências aplicáveis ao produto que contêm, ou recicladas, se a reutilização não for possível.

5. GARANTIA DE ADEQUAÇÃO DO PRODUTO

5.1. A Contratada deverá oferecer garantia, pelo prazo constante na descrição de cada item, contra qualquer vício de fabricação e montagem/instalação, a partir do recebimento definitivo.

5.2. A Contratada deverá assegurar o cumprimento da garantia/assistência técnica **por parte do fabricante**, durante o respectivo período de vigência, sem ônus adicionais para o Contratante; caso não sejam prestadas na forma contemplada pelo TR, fica a Contratada sujeita às penalidades insculpidas no item 8.

5.3 A Contratada obriga-se a efetuar o atendimento aos chamados para prestação de assistência técnica decorrente da garantia, **no prazo máximo constante na descrição de cada item** a partir do recebimento da comunicação.

5.4. A Contratada deverá apresentar, a cada procedimento de assistência técnica, relatório de visita contendo a data do recebimento do chamado, a identificação do vício constatado e as providências tomadas ou a serem adotadas, informando o prazo necessário para concluir a assistência, que não poderá ser superior a 30 dias, contados da data do recebimento do chamado.

5.5 Não sendo o vício sanado no prazo do subitem 5.4, a fiscalização do contrato notificará a contratada para que substitua o produto por outro novo da mesma espécie, marca e modelo, em perfeitas condições de uso, em no máximo **60 dias**, contados da notificação, sob pena de serem-lhe aplicadas as sanções previstas no edital e no contrato.

6. OBRIGAÇÕES DA CONTRATADA

6.1. São obrigações da Contratada, além daquelas explícita ou implicitamente contidas no presente termo de referência e na legislação vigente:

a) entregar os bens no prazo, nas especificações e na quantidade constantes neste termo de referência, assim como com as características descritas na proposta;

b) atender às solicitações do Contratante nos prazos estabelecidos neste instrumento;

c) não fornecer quantidade ou modelo diversos do solicitado;

d) substituir os produtos danificados em razão de transporte, descarga ou outra situação que não possa ser imputada à Administração;

e) responder pelos encargos previdenciários, trabalhistas, fiscais e comerciais resultantes da execução do contrato;

f) responder por quaisquer danos pessoais ou materiais causados por seus empregados à Administração e/ou a terceiros na execução deste Contrato;

g) manter, durante a execução do ajuste, todas as condições de habilitação exigidas para a contratação;

h) reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções;

i) não subcontratar, ceder ou transferir, no todo ou em parte, o objeto do contrato, salvo se autorizado neste termo de referência;

j) prestar garantia de adequação dos produtos (qualidade, segurança, durabilidade e desempenho), em conformidade com as condições estabelecidas neste termo de referência.

7. OBRIGAÇÕES DO CONTRATANTE

7.1. A Contratante obriga-se a:

a) acompanhar e fiscalizar a execução do ajuste, anotando em registro próprio as ocorrências acaso verificadas, determinando o que for necessário à regularização das faltas ou defeitos observados;

b) prestar esclarecimentos que venham a ser solicitados pela Contratada;

c) efetuar os pagamentos nas condições e nos prazos constantes neste termo de referência e no edital;

d) zelar para que, durante a vigência do Contrato, a Contratada cumpra as obrigações assumidas, bem como sejam mantidas as condições de habilitação e qualificação exigidas no processo licitatório;

e) determinar a reparação, a correção, a remoção ou a substituição do objeto do contrato em que se verificarem vícios, defeitos ou incorreções.

8. INADIMPLEMENTO E PENALIDADES

8.1 A Administração poderá aplicar à licitante vencedora, pelo descumprimento total ou parcial das obrigações assumidas, as sanções previstas na Lei e no Contrato, sendo a multa calculada dentro dos seguintes parâmetros:

a) atrasar injustificadamente a entrega do objeto contratado – 1**%, sobre o valor do material entregue em atraso, por dia de atraso, até o máximo de 20 dias;**

b) inexecução parcial – **20% sobre o valor do material não entregue;**

c) inexecução total – **30% sobre o valor total contratado;**

d) atrasar, até no máximo **2 dias úteis**, o atendimento para prestar assistência técnica decorrente da garantia, a correção do vício ou a substituição do produto – **0,5% do valor de aquisição do bem, para o qual foi solicitada a assistência técnica, por dia de atraso;**

e) não atender ao chamado para prestar assistência técnica, decorrente da garantia, ou não substituir o bem que apresentou, dentro do prazo de garantia, vícios que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor – **30% do valor total de aquisição do material não substituído.**

8.2. Ultrapassado o prazo estabelecido no **subitem 8.1, alínea "a",** a Administração poderá não receber os itens pendentes de entrega.

8.3. A aplicação da penalidade estabelecida no **subitem 8.1, alínea "e"** não afasta a obrigação de substituição do bem ou do pagamento do seu equivalente.

9. MEDIDAS ACAUTELADORAS

9.1. Ocorrendo inadimplemento contratual, a Administração poderá, com base no artigo 45 da Lei nº 9.784/1999 e artigo 7º, parágrafo único, da Portaria nº 455/2016, do TRE/BA, reter de forma cautelar, dos pagamentos devidos à Contratada, valor relativo a eventual multa a ser-lhe aplicada.

9.2. Finalizado o processo administrativo de apuração das faltas contratuais cometidas pela Contratada, tendo a Contratante decidido pela penalização, o valor retido cautelarmente será convertido em multa. Não havendo decisão condenatória, o valor será restituído, monetariamente corrigido pelo mesmo índice de reajuste dos pagamentos devidos à Contratada.

10. PAGAMENTO

10.1. Observada a ordem cronológica estabelecida no art. 5º da Lei 8.666/93, o pagamento será efetuado sem qualquer acréscimo financeiro, mediante depósito através de ordem bancária, nos seguintes prazos e condições:

10.1.1. Para valor igual ou inferior a R$ 17.600,00: até o 5º dia útil subsequente à apresentação da nota fiscal;

10.1.2. Para valor superior a R$ 17.600,00: até o 10º dia útil subsequente à apresentação da nota fiscal.

10.2. Condiciona-se o pagamento à:

I – Apresentação da nota fiscal discriminativa da execução do objeto contratado;

II – Declaração da Fiscalização do Contrato de que o fornecimento se deu conforme pactuado.

10.3. A Contratada indicará na nota fiscal o nome do Banco e os números da agência e da conta corrente para efetivação do pagamento.

10.4. A Contratante, observados os princípios do contraditório e da ampla defesa, poderá deduzir, do montante a pagar à Contratada, os valores correspondentes a multas, ressarcimentos ou indenizações por esta devidos.

11. CRITÉRIOS DE SUSTENTABILIDE

11.1. Para os equipamentos dos itens 1 a 6, a Contratada deverá comprovar que o fabricante possui programa instituído de recolhimento adequado de eletrônicos com destinação à reciclagem, em conformidade a Resolução 201/2015 do CNJ.

11.2. Para os equipamentos dos itens 1 a 6, a Contratada deverá fornecer equipamentos embalados em material reciclável.

TRIBUNAL REGIONAL ELEITORAL DA BAHIA

ANEXO A

ESPECIFICAÇÕES DETALHADAS

ITEM	ESPECIFICAÇÕES DETALHADAS
1	**COMUTADOR CENTRAL** **<u>Marca: CISCO. Modelo: Nexus, com as seguintes configurações:</u>** 1. CARACTERÍSTICAS GERAIS 1.1. Equipamento com operação na camada 3 do modelo OSI (Layer 3); 1.2. O equipamento deve possuir instalada, no mínimo, a seguinte configuração de portas: 1.3. Deve possuir 6 (seis) portas com suporte a 40 e 100 Gigabit Ethernet conforme padrão QSFP28; 1.4. Deve permitir a utilização de cabos breakout nestas portas para conversão de uma determinada interface em quatro conexões de 10GbE; 1.5. Deve possuir 48 (quarenta e oito) interfaces SFP+ para conexão de fibras ópticas monomodo ou multimodo com velocidades de 1, 10 e 25 Gigabit Ethernet; 1.6. O switch deve implementar non-blocking wire speed em todas as portas; 1.7. Deve acompanhar 1 (um) cabo de conexão direta em 40GbE com, no mínimo, 5 (cinco) metros; 1.8. Deve possuir gabinete de no máximo 01 (um) RU (rack unit) e permitir instalação em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários; 1.9. Possuir porta de console para ligação direta, de terminal RS-232 ou RJ-45 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB; 1.10. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implantação de todas as funcionalidades descritas nesta especificação; 1.11. Permitir o encaminhamento de “jumbo frames” em todas as portas (pacotes de 9000 bytes); 1.12. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática. Deve incluir fonte de alimentação redundante. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136; 1.13. Deverá ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas; 1.14. Possuir LEDs para a indicação do status das portas e atividade; 1.15. A ventilação do equipamento deverá seguir o fluxo onde o ar entra através das portas e com exaustão através das fontes; 1.16. Possuir capacidade para pelo menos 128.000 (noventa mil) endereços MAC na tabela de comutação; 1.17. Possuir backplane de, no mínimo, 3.6 Tbps (Terabits por segundo); 1.18. O equipamento deve ter capacidade mínima de encaminhamento de 1.5 Bpps (Bilhões de pacotes por segundo); 2. GERENCIAMENTO 2.1. Implementar os padrões abertos de gerência de rede SNMP (v1, v2 e v3), incluindo a geração de traps; 2.2. Suportar SNMP sobre IPv6; 2.3. Possuir suporte a MIB II, conforme RFC 1213; 2.4. Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento;

	2.5. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa; 2.6. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas; 2.7. Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas; 2.8. Implementar nativamente grupos RMON Alarms e Events; 2.9. Ser configurável e gerenciável via CLI (command line interface), Telnet e SSH; 2.10. Permitir que a configuração seja realizada através de terminal assíncrono; 2.11. Permitir a gravação de log externo (syslog); 2.12. Possuir 1 (uma) porta 10/100/1000BaseT, com conector RJ-45, exclusivamente para gerência do equipamento. Esta porta será conectada na rede de gerência e o switch deverá permitir a configuração de endereço IP próprio para gerenciamento; 2.13. O equipamento deve permitir sua configuração através de NETCONF; 2.14. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace e log de eventos; 3. FACILIDADES 3.1. Permitir a agregação de, no mínimo, 08 (oito) portas segundo o padrão IEEE 802.3ad; 3.2. Deve permitir a criação de links de agregação entre interfaces de dois equipamentos separados e idênticos, especificados nesta seção do edital, e pelo menos duas interfaces de um terceiro dispositivo que suporte 802.3ad, este que tratará o link redundante de forma transparente como se estivesse conectado a um único equipamento. Esta funcionalidade também é conhecida como Multi-Chassis Link Agregation, MultiChassis Etherchannel, Multi-Switch Link Aggregation (M-LAG) ou Virtual PortChannel; 3.3. Implementar VLANs compatíveis com o padrão IEEE 802.1q. Deve implementar, no mínimo, 3.000 (três mil) VLANs simultaneamente; 3.4. Permitir o espelhamento do tráfego total de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch, localizada em outro switch do mesmo tipo conectado à mesma rede local, ou mesmo, localizada em um switch do mesmo tipo com endereço IP remoto; 3.5. Permitir a virtualização das tabelas de roteamento em camada 3 através de VRFs “Virtual Routing and Forwarding” ou VRF-Lite; 3.6. Implementar o protocolo NTP (Network Time Protocol); 3.7. Deve suportar a autenticação dos servidores NTP; 3.8. Deve suportar o protocolo IPv6; 3.9. Deve implementar os protocolos Device Link Detection Protocol (DLDP) ou Unidirectional Link Detection (UDLD) para detecção de tráfego unidirecional com o objetivo de prevenir loops na rede; 3.10. Deve implementar DHCP Relay ou UDP Helper; 3.11. Deve implementar Virtual Extensible LAN (VXLAN); 4. ROTEAMENTO 4.1. Implementar roteamento estático IPv4 e IPv6; 4.2. Implementar roteamento dinâmico RIPv2 conforme as RFCs 2082 e 2453; 4.3. Implementar protocolo de roteamento dinâmico OSPF conforme as RFCs 2328, 2370, 2740, 3101, 3137 e 3623; 4.4. Implementar protocolo de roteamento BGPv4 conforme as RFCs, 1997, 2385, 3065, 4271 e 4456); 4.5. Implementar protocolo de roteamento EIGRP; 4.6. Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway; 4.7. Implementar simultaneamente, no mínimo, 255 (duzentos e cinquenta e cinco) grupos do VRRP ou do mecanismo similar de redundância de gateway; 4.8. Implementar roteamento baseado em política (Policy-based Routing);

	4.9. Implementar Equal-Cost Multipath (ECMP) para permitir a criação de múltiplas rotas para o mesmo destino; 5. SEGURANÇA 5.1. Implementar mecanismo de AAA (Authentication, Authorization e Accounting) para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+ ou RADIUS; 5.2. Deve permitir a criação de listas de acesso (ACLs), internamente ao equipamento, baseadas em endereço IP de origem, endereço IP de destino, portas TCP e UDP, campo DSCP e horário (dia e hora); 5.3. Deve implementar filtragem de pacotes IPv6 através de Access Control List (ACL); 5.4. Deve ser possível habilitar o log das ACLs IPv4; 5.5. Possibilitar a autenticação da sessão SSH através de certificado digital; 5.6. Implementar funcionalidade para controle do volume de tráfego unicast, multicast e broadcast de uma interface, atribuindo porcentagens permitidas para cada um dos tráfegos; 5.7. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha; 5.8. Implementar mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques no ambiente nível 2; 5.9. Implementar mecanismo para suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em uma determinada porta do switch; 6. PADRÕES 6.1. Implementar padrão IEEE 802.1d (Spanning Tree Protocol); 6.2. Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol); 6.3. Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 50 (cinquenta) instâncias simultâneas do protocolo Spanning-Tree; 6.4. Implementar padrão IEEE 802.1Q (Vlan Frame Tagging); 6.5. Implementar padrão IEEE 802.1p (Class of Service); 6.6. Implementar padrão IEEE 802.3ad (LACP); 6.7. Permitir a descoberta de outros dispositivos na rede de forma automática através do protocolo LLDP (IEEE 802.1AB) ou semelhantes; 6.8. Implementar o protocolo PTP (Precision Time Protocol) de acordo com a IEEE 1588; 6.9. Deve suportar o protocolo VTP (Vlan Trunking Protocol) para compartilhamento de VLAN com os switches marca Cisco já existentes neste órgão; 7. MULTICAST 7.1. Implementar mecanismo de controle de multicast através de IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376); 7.2. Implementar o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch; 7.3. Implementar roteamento multicast através do protocolo PIM (Protocol Independent Multicast) no modo “sparse-mode” conforme RFC 3569; 8. QUALIDADE DE SERVIÇO (QoS) 8.1. Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p; 8.2. Deve permitir a classificação do tráfego em classes utilizando como base os seguintes métodos: Listas de controle de acessos (ACL), campo CoS (Class of Service), DSCP (Differentiated Services Code Point) e IP Precedence; 8.3. Uma vez classificado o tráfego, o equipamento deve marcar os seguintes campos: Class of Service (CoS), Differentiated Services Code Point (DSCP) e IP Precedence; 8.4. O equipamento deve implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: WRED (Weighted Random Early Detection) ou Weighted Fair

Queuing (WFQ);
8.5. Deve suportar o mecanismo Explicit Congestion Notification (ECN);
8.6. Deve suportar Priority Flow Control (PFC) conforme o padrão IEEE 802.1Qbb.

9. COMPATIBILIDADE
9.1. Este equipamento deverá ser plenamente compatível com os equipamentos e acessórios CISCO existentes no ambiente da contratante;
9.2. Deve ser possível adicionar este equipamento ao sistema de gerenciamento CISCO Prime Infrastructure já existente no ambiente da contratante. Caso necessário, deve acompanhar as licenças necessárias para inclui-lo ao software de gerenciamento CISCO Prime Infrastructure.

10. SERVIÇO DE SUPORTE TÉCNICO
10.1. A CONTRATADA deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, *website* e e-*mail*;
10.2. O registro da solicitação pode ser realizado através de contato telefônico, disponibilizado 24 horas por dia, 7 dias por semana, com o primeiro atendimento em até 4 horas úteis;
10.3. As ligações deverão ser gratuitas, adotando-se o sistema 0800;
10.4. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de chamados de suporte técnico;
10.5. A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;
10.6. Os chamados abertos por e-mail deverão ter sua abertura automática no portal web;
10.7. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;
10.8. A contratada deverá prestar o suporte técnico dos produtos fornecidos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações à contratante;
10.9. A contratada deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico;
10.10. A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante;
10.11. As atualizações incluídas devem ser do tipo “minor release” e “major release”, permitindo manter os equipamentos atualizados em sua última versão de software/firmware;

11. GARANTIA
11.1. A garantia do equipamento deverá ser de 36 meses com tempo de solução de chamados, incluindo envio de peças e equipamento de reposição de até 5 dias úteis;
11.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos;
11.3. Os softwares fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório dos softwares;
11.4. A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição. Obrigatoriamente o envio de peças/equipamentos de reposição deve ser realizado pelo fabricante dos equipamentos, sendo este responsável pelo controle e logística de peças de reposição.

2	**COMUTADOR DE BORDA** **<u>Marca: CISCO. Modelo: Catalyst 2960, com as seguintes configurações:</u>** 1. CARACTERÍSTICAS GERAIS 1.1. Equipamento tipo comutador gigabit ethernet com capacidade de operação em camada 3 do modelo OSI; 1.2. Deve ser fornecido com 48 (quarenta e oito) portas 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45; 1.3. Deve prover alimentação PoE+ conforme o padrão IEEE 802.3at nas 48 (quarenta e oito) portas 1000Base-T, com 370W exclusivos para alimentação PoE, a serem alocados em todas as portas. Não serão aceitas fontes externas ou módulos adicionais para alimentação PoE; 1.4. Deve ser fornecido com 2 slots para conexão de transceivers SFP/SFP+ para fibras ópticas multimodo e monomodo com velocidade de 1GbE/10GbE. Estas portas devem ser de uso simultâneo com as portas 1000Base-T e não serão aceitas interfaces do tipo combo; 1.5. Deve possuir 50 portas ethernet ativas simultaneamente, não incluindo interfaces de empilhamento; 1.6. Deve suportar empilhamento através de interfaces dedicadas, com velocidade mínima de 80 Gbps, configurado em forma de anel, formando pilhas de pelo menos 8 unidades e compatível com os switches marca Cisco, modelo 2960X já existentes neste órgão. Deve-se utilizar portas específicas para este fim, de uso traseiro; 1.7. Deve empilhar com switches PoE e não PoE. Os switches PoE devem prover alimentação conforme o padrão 802.3at, fornecendo até 30W por porta; 1.8. Deve permitir a criação de links agrupados virtualmente (link aggregation) utilizando portas de diferentes switches da pilha; 1.9. Deve possuir porta de console frontal para total gerenciamento local, com conector RS-232, RJ-45 ou USB; 1.10. Deve possuir capacidade de vazão de pelo menos 120 mpps; 1.11. Deve possuir funcionalidade que permita o autodescobrimento do equipamento conectado na porta do switch. Após este descobrimento, o switch deve aplicar sem intervenção humana as configurações na porta (VLAN, velocidade, QoS) conforme o tipo de equipamento conectado. A detecção do equipamento conectado deve ocorrer de forma automática; 1.12. O equipamento deve permitir sua configuração automática com base em outro equipamento da rede, sem intervenção humana, permitindo a sua rápida substituição. Ao ser ligado, o equipamento deve buscar esta configuração em outro equipamento da rede, utilizando-se para isso parâmetros fornecidos pelo DHCP; 1.13. Deve permitir o espelhamento do tráfego de uma porta (port mirroring) para outra porta do mesmo switch ou para uma porta de outro switch que estiver na rede. Deve permitir ainda o espelhamento de tráfego nos switches marca Cisco, modelo 2960X já existentes neste órgão; 1.14. Deve possuir Jumbo Frame de pelo menos 9000 bytes; 1.15. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, permitindo a criação de no mínimo 1000 VLANs com IDs entre 1 e 4000; 1.16. Deve implementar roteamento IP (Layer 3) com pelo menos 4 interfaces roteáveis, permitindo a criação de pequenos backbones; 1.17. Deve permitir a criação de links agrupados virtualmente (link aggregation); 1.18. Permitir a descoberta de outros dispositivos na rede de forma automática através do protocolo LLDP (IEEE 802.1AB) ou semelhantes; 1.19. Deve possuir IGMP snooping para controle de tráfego de multicast; 1.20. Deve suportar Multicast VLAN, de forma que o tráfego Multicast da rede seja isolado em uma VLAN diferente das demais; 1.21. Deve implementar MLD v1 e v2; 1.22. Deve identificar automaticamente portas em que telefones IP estejam conectados e associá-las

automaticamente a VLAN de voz;

1.23. Deve implementar Spanning Tree por vlan e conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree) com filtros BPDU. Deve implementar pelo menos 32 instâncias de Multiple Spanning Tree;

1.24. Deve possuir priorização de pacotes (QoS) com 8 (oito) filas de prioridade por porta. Deve implementar a classificação de pacotes com base em regras de ACL;

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

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

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

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

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

1.30. Deve implementar IPv6 com as seguintes RFCs: 1981, 2373, 2460, 2461, 2462 e 2463;

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

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

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

1.34. Deve responder a pacotes para teste de rede, suportando no mínimo as seguintes operações de teste: TCP connect e UDP echo. Caso o equipamento ofertado não forneça essa funcionalidade, deve ser fornecida ferramenta capaz de prover estas funcionalidades;

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

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

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

1.38. Deve permitir a criação de três níveis de administração e configuração do switch. Deve permitir a autenticação de usuário de gerência em servidor RADIUS e TACACS;

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

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

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

1.42. Deve suportar o protocolo VTP (Vlan Trunking Protocol) para compartilhamento de VLAN com os switches marca Cisco já existentes neste órgão;

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

1.44. Deve suportar fonte de alimentação redundante;

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

2. MÓDULO DE EMPILHAMENTO

2.1. 2. Deve vir acompanhado de interface de empilhamento, com as seguintes características:

	2.1.1. Deve ser *hot-swappable*; 2.1.2. 3. Deve possuir 2 (duas) interfaces de uso exclusivo para empilhamento, totalizando 80Gbps de velocidade na pilha; 2.1.3. 4. Deve permitir o empilhamento de até 8 (oito) unidades na pilha de comutadores; 2.1.4. 5. Deve vir acompanhado de pelo menos 1 (um) cabo com 0,5m de comprimento específico para empilhamento; 3. COMPATIBILIDADE 3.1. Este equipamento deverá ser plenamente compatível com os equipamentos e acessórios CISCO existentes no ambiente da contratante; 3.2. Deve ser possível adicionar este equipamento ao sistema de gerenciamento CISCO Prime Infrastructure já existente no ambiente da contratante. Caso necessário, deve acompanhar as licenças necessárias para inclui-lo ao software de gerenciamento CISCO Prime Infrastructure. 4. SERVIÇO DE SUPORTE TÉCNICO 4.1. A CONTRATADA deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, *website* e e-*mail*; 4.2. O registro da solicitação pode ser realizado através de contato telefônico, disponibilizado 24 horas por dia, 7 dias por semana, com o primeiro atendimento em até 4 horas úteis; 4.3. As ligações deverão ser gratuitas, adotando-se o sistema 0800; 4.4. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de chamados de suporte técnico; 4.5. A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema; 4.6. Os chamados abertos por e-mail deverão ter sua abertura automática no portal web; 4.7. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk; 4.8. A contratada deverá prestar o suporte técnico dos produtos fornecidos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações à contratante; 4.9. A contratada deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico; 4.10. A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante; 4.11. As atualizações incluídas devem ser do tipo “minor release” e “major release”, permitindo manter os equipamentos atualizados em sua última versão de software/firmware; 5. GARANTIA 5.1. A garantia do equipamento deverá ser de 36 meses com tempo de solução de chamados, incluindo envio de peças e equipamento de reposição de até 5 dias úteis; 5.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos; 5.3. Os softwares fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório dos softwares; 5.4. A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição. Obrigatoriamente o envio de peças/equipamentos de reposição deve ser realizado pelo fabricante dos equipamentos, sendo este responsável pelo

	controle e logística de peças de reposição.
3	**TRANSCEIVER 10GBASE-LR** **<u>Marca: CISCO. Modelo: SFP-10G-LR, com as configurações técnicas a seguir:</u>** 1. CARACTERÍSTICAS GERAIS 1.1. Transceiver SFP+ para conexão de fibras ópticas monomodo; 1.2. Deve ser compatível com o padrão 10GBase-LR para fibras ópticas de até 10km; 1.3. Deve possuir conector LC; 1.4. Deve possuir velocidade de 10GbE; 1.5. Deve ser do mesmo fabricante e homologado pelo fabricante para funcionar com os comutadores dos itens 1 e 2 deste processo. 2. SERVIÇO DE SUPORTE TÉCNICO 2.1. A CONTRATADA deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, website e e-mail; 2.2. O registro da solicitação pode ser realizado através de contato telefônico, disponibilizado 24 horas por dia, 7 dias por semana, com o primeiro atendimento em até 4 horas úteis; 2.3. As ligações deverão ser gratuitas, adotando-se o sistema 0800; 2.4. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de chamados de suporte técnico; 2.5. A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema; 2.6. Os chamados abertos por e-mail deverão ter sua abertura automática no portal web; 2.7. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk; 3. GARANTIA 3.1. A garantia do transceiver deverá ser de 36 meses ou deve herdar o prazo do equipamento ao qual está instalado com tempo de solução de chamados, incluindo envio de peças e equipamento de reposição de até 5 dias úteis; 3.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos; 3.3. A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição. Obrigatoriamente o envio de peças/equipamentos de reposição deve ser realizado pelo fabricante dos equipamentos, sendo este responsável pelo controle e logística de peças de reposição.
4	**TRANSCEIVER 10GBASE-SR** **<u>Marca: CISCO. Modelo: SFP-10G-SR, com as seguintes configurações:</u>**

	1. CARACTERÍSTICAS GERAIS 1.1. Transceiver SFP+ para conexão de fibras ópticas multimodo; 1.2. Deve ser compatível com o padrão 10GBase-SR para fibras ópticas de até 300m (OM3); 1.3. Deve possuir conector LC; 1.4. Deve possuir velocidade de 10GbE; 1.5. Deve ser do mesmo fabricante, e homologado pelo fabricante para funcionar com os comutadores dos itens 1 e 2 deste processo. 2. SERVIÇO DE SUPORTE TÉCNICO 2.1. A CONTRATADA deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, website e e-mail; 2.2. O registro da solicitação pode ser realizado através de contato telefônico, disponibilizado 24 horas por dia, 7 dias por semana, com o primeiro atendimento em até 4 horas úteis; 2.3. As ligações deverão ser gratuitas, adotando-se o sistema 0800; 2.4. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de chamados de suporte técnico; 2.5. A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema; 2.6. Os chamados abertos por e-mail deverão ter sua abertura automática no portal web; 2.7. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk; 3. GARANTIA 3.1. A garantia do transceiver deverá ser de 36 meses ou deve herdar o prazo do equipamento ao qual está instalado com tempo de solução de chamados, incluindo envio de peças e equipamento de reposição de até 5 dias úteis; 3.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos; 3.3. A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição. Obrigatoriamente o envio de peças/equipamentos de reposição deve ser realizado pelo fabricante dos equipamentos, sendo este responsável pelo controle e logística de peças de reposição.
5	**COMUTADOR DE CARTÓRIO** **<u>Modelos de Referência: CISCO SF220-26P, HPE J9983A, TP-LINK TL-SG2424P, D-LINK DGS-1510-28P e Intelbras SG2404 PoE 24 portas</u>** 1. CARACTERÍSTICAS GERAIS 1.1. Equipamento tipo comutador gigabit ethernet com capacidade de operação em camada 2 do modelo OSI;

	1.2. Deve ser fornecido com, no mínimo, 16 (dezesseis) portas, IEEE 802.3u 100BASE-TX Fast Ethernet ou IEEE 802.3ab 1000BASE-T Gigabit Ethernet, para conexão de cabos de par metálico UTP com conector RJ-45. Deve suportar Auto-MDIX e negociação automática de speed e duplex; 1.3. Deve prover alimentação PoE+ conforme o padrão IEEE 802.3at em, no mínimo 8 (oito) portas, com 180W exclusivos para alimentação PoE+, a serem alocados em todas as portas; 1.4. Deve possuir capacidade de vazão (taxa de encaminhamento) de pelo menos 26 (vinte e seis) Mpps; 1.5. Deve ser equipamento de linha de produção atual do fabricante; 1.6. Deve possuir site do fabricante na Internet com descritivo de suas especificações técnicas; 1.7. Deve possuir tabela para, no mínimo, 8.000 (oito mil) endereços MAC; 1.8. Deve possuir Jumbo Frame de pelo menos 9000 bytes; 1.9. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, permitindo a criação de no mínimo 60 VLANs; 1.10. Deve possuir o protocolo “Network Time Protocol” (NTP), autenticado, para a sincronização do relógio com outros dispositivos de rede; 1.11. Deve permitir configuração/administração remota através de SSH ou GUI Web HTTPS, e através de SNMPv3; 1.12. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136; 1.13. Gabinete padrão para montagem em rack de 19" ou *half width rack*, com altura máxima de 1U, incluindo todos os acessórios para o perfeito funcionamento; 2. SERVIÇO DE SUPORTE TÉCNICO 2.1. O suporte técnico do fabricante deverá ser provido por meio de telefone, website e e-mail; 2.2. Deverá haver assistência técnica local, ou seja, na cidade do endereço de entrega (Salvador-BA); 2.3. O fabricante deverá possibilitar o acompanhamento dos registros de suporte; 2.4. O fabricante deverá disponibilizar todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período de garantia, sem qualquer ônus adicional para o contratante; 3. GARANTIA 3.1. A garantia do equipamento deverá ser do tipo padrão de balcão por, no mínimo, 12 (doze) meses; 3.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período de garantia, a contar da data do recebimento definitivo dos equipamentos; 3.3. O fabricante deverá disponibilizar atualização dos softwares inerentes ao equipamento fornecido de modo a possibilitar correção de vícios ou falhas de segurança.
6	**SOLUÇÃO UNIFICADA DE SEGURANÇA** **<u>Marca: Check Point. Modelo: Check Point 5600, com as configurões técnicas a seguir:</u>** 1. CARACTERÍSTICAS GERAIS 1.1. Por funcionalidades de NG - Next Generation Threat Prevention, entende-se: controle granular de aplicações e URL, identificação de usuários, Antivirus e Antibot, Emulação e Extração de Ameaças, IPS e Firewall; 1.2. 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; 1.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; 1.4. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura; 1.5. Todos os equipamentos deverão ser gerenciados através da mesma console de gerenciamento atualmente em uso no TRE-BA para gerenciamento dos equipamentos responsáveis pela comunicação com o TSE ; 1.6. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução. 1.7. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3. 1.8. O Gateway de Segurança deve ser capaz de suportar as seguintes funcionalidades gerenciamento unificado de aplicações em uma única plataforma: 1.8.1. Stateful Inspection Firewall 1.8.2. Intrusion Prevention System 1.8.3. User Identity Acquisition 1.8.4. Application Control and URL filtering 1.8.5. AntiBot e AntiVirus 1.8.6. Threat Emulation (Sandboxing) 1.8.7. AntiSpam and Email Security 1.8.8. IPSec VPN 1.8.9. Data Loss Prevention 1.8.10. Mobile Access 1.8.11. Security Policy Management 1.8.12. Logging and Status 1.8.13. Event Correlation and Reporting 1.9. A solução deverá prover conscientização do usuário final de acordo com as políticas de segurança em tempo real; 1.10. A Solução deverá prover inspeção SSL: 1.11. A solução deverá suportar PFS (Perfect Forward Secrecy) e suítes ECDHE de criptografia; 1.12. A solução deverá possuir suporte para AES-NI, AES-GCM com a finalidade de aumentar o desempenho; 1.13. O hardware e software fornecido não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. 2. CARACTERÍSTICAS FÍSICAS 2.1. Tamanho máximo de 2U por equipamento; 2.2. Cada appliance de segurança, deverá possuir no mínimo os seguintes throughput: 2.2.1. Throughput de 25 (vinte e cinco) Gbps para a funcionalidade de firewall; 2.2.2. Throughput de 7 (sete) Gbps para a funcionalidade de IPS; 2.2.3. Throughput de 6 (seis) Gbps para funcionalidade de VPN com algoritmo AES-128; 2.2.4. Sendo que o appliance não deve sofrer degradação de performance quando as funcionalidades de Firewall, Controle de aplicação WEB e IPS tiverem habilitadas de forma simultânea, sendo que o trafego deverá ser inspecionado de modo bidirecional e a inspeção deve ser feita para toda a sessão do pacote, sem qualquer utilização de feature de bypass do pacote/sessão. 2.3. Possuir alimentação elétrica a partir de, no mínimo, 02 (duas) fontes independentes, redundantes e hotswap, capazes de operar entre 100 a 120VAC e entre 200 e 240VAC, por reconhecimento automático do nível de tensão; 2.4. Deve possuir 10 (dez) interfaces de rede 10/100/1000 base-TX; 2.5. A solução deve suportar até 04 (quatro) interfaces 10 Gigabit SFP+; 2.6. Possuir, no mínimo, 01 (uma) interface de rede 10/100/1000 Gbps deve ser dedicada para o gerenciamento, podendo ser utilizada uma das interfaces do subitem 2.4;

	2.7. Possuir, no mínimo, 01 (uma) interface do tipo console ou similar; 2.8. Possuir, no mínimo, 01 (uma) interface de rede 10/100/1000 Gbps dedicada para alta disponibilidade, podendo ser utilizada uma das interfaces do subitem 2.4; 2.9. Possuir interface de gerenciamento do tipo LOM; 2.10. A solução deve possuir disco rígido de, no mínimo, 200 GB sendo ele do tipo SSD (Solid-Stade Drive); 3. CONTROLE DE POLÍTICAS DE *FIREWALL* 3.1. A solução deve incluir *appliance* do próprio fabricante ou servidores Open Server de outros fabricantes sendo eles listados em uma base de compatibilidade de hardware. 3.2. Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado; 3.3. O sistema operacional da solução deverá ser customizado pelo próprio fabricante do *firewall* para garantir segurança e melhor desempenho ao firewall, permitindo o monitoramento de recursos no *appliance*; 3.4. Deve suportar atuação como cliente NTP (Network Time Protocol) versão 1, 2, 3 e 4; 3.5. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede; 3.6. O hardware deve ser baseado em arquitetura aberta usando processadores Intel ou AMD a fim de manter flexibilidade e adaptação a novas ameaças sem impacto na performance; 3.7. Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar pelo menos 1024 (mil e vinte e quatro) sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas; 3.8. A comunicação entre a solução de gerência e os *appliances* de segurança deverá ser criptografada, sendo que a comunicação entre eles deve ser protegida através de uma Infraestrutura de Chaves Públicas interna do próprio fabricante da Solução ofertada; 3.9. Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos; 3.10. A solução deve permitir que em caso de falha de comunicação entre o *appliance* de segurança e a solução de armazenamento de *logs* seja possível a retenção temporária na mesma unidade física de armazenamento do sistema operacional do *appliance* de segurança; 3.11. A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos, permitindo a pesquisa dos mesmos em todo o log orientado aos sentidos vertical, horizontal e transversal, sendo necessária apenas a informação da *string* de texto no campo de pesquisa para que seja feito o filtro dos eventos NGFW de forma agregada e multidisciplinar (trazendo a trilha das diversas funcionalidades relacionadas a esta pesquisa); 3.12. As regras deverão ser construídas utilizando objetos de rede baseadas no protocolo IP. Durante a criação da regra, tais objetos deverão ser associados automaticamente às suas interfaces de rede correspondentes, sem que haja necessidade de o administrador associar, na regra, qual é a interface de rede origem da conexão, nem a interface de rede destino da conexão. Não será aceito definição de interface com a variável “any”; 3.13. Deve suportar a implementação de monitoração de links Internet, através do teste de conectividade com endereços específicos e implementar alertas em caso de quedas. 3.14. Deverá possibilitar a implementação de balanceamento de *links* em modos de Ativo/Ativo ou Ativo/Passivo. 3.15. Após uma queda da conexão primária, quando essa retornar deve ser possível configurar as ações como por exemplo alertas de SNMP, log, scripts customizados pelo usuário. 3.16. Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP; 3.17. A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: Tokens (como SecurID), TACACS, RADIUS, certificados digitais e dispositivos biométricos 3.18. Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora; 3.19. Em caso de falhas nas rotas primárias deve desviar dinamicamente o tráfego para um link secundário, roteamento com base em prioridades; 3.20. Implementar roteamento e encaminhamento baseado em políticas;

	3.21. Deve implementar roteamento *multicast* (PIM-SM); 3.22. Possuir funcionalidade de DHCP Relay e DHCP Server; 3.23. Suporte à criação de objetos de rede, sendo que um mesmo objeto possa ser utilizado com endereço IP nas versões 4 e 6 simultaneamente a este mesmo objeto que será associado à base de regras; 3.24. Possuir base de regras singular sem separação de regras orientadas a versão de endereço IP utilizada; 3.25. Prover a otimização administrativa e lógica quando referenciado há um mesmo host com as duas versões do endereço IP sem a multiplicação de objetos e regras; 3.26. Implementar sub-interfaces ethernet lógicas; 3.27. Deve suportar os seguintes tipos de NAT: 3.27.1. Nat dinâmico (Many-to-1); 3.27.2. Nat dinâmico (Many-to-Many); 3.27.3. Nat estático (1-to-1); 3.27.4. NAT estático (Many-to-Many); 3.27.5. Nat estático bidirecional 1-to-1; 3.27.6. NAT de Origem; 3.27.7. NAT de Destino; 3.28. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção; 3.29. Deve implementar roteamento estático IPv4 e IPV6; 3.30. Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4; 3.31. Deve implementar roteamento dinâmico (OSPFv3) para IPv6; 3.32. Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing); 3.33. Deve suportar no mínimo as seguintes funcionalidades: 3.33.1. A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através de padrões de análise de protocolo tais como de Tipo de Protocolo ou Inspeção de SSH; 3.33.2. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound); 3.33.3. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2; 3.34. Deve ter a capacidade de inspecionar e bloquear tráfego operando nos seguintes modos: camada 2 (l2) e camada 3 (l3); 3.35. Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações; 3.36. Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações. 3.37. Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade); 3.38. Na ocorrência de falhas, as conexões existentes em um firewall deverão ser mantidas pelo (s) outro (s) sem perdas destas conexões, não acarretando interrupções no tráfego da rede; 3.39. Na aplicação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas; 3.40. Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar as informações armazenadas para realizar autenticações; 3.41. Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS; 3.42. A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização; 3.43. A solução não deve por "default" permitir que todas as portas TCP/UDP resultem em um estado do tipo "open" após um "scan ports"; 3.44. Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;

	3.45. Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora; 3.46. Deverá suportar métodos de autenticação de usuário, cliente e sessão; 3.47. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando existirem múltiplos executando alterações simultaneamente; 3.48. Habilidade de realizar upgrade via SCP ou https via interface WEB; 3.49. A solução de segurança deve possuir capacidade de endereços MAC trafegados superior a 4.000 endereços; 3.50. A solução deverá disponibilizar uma ferramenta onde o fabricante disponibilize HotFixes de segurança e upgrades de versão para instalação simples e com zero-downtime; 3.51. Possuir funcionalidade de HTTP e HTTPS proxy. 4. ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA 4.1. Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: 4.1.1. Em modo Transparente: 4.1.2. Em Layer 2; 4.1.3. Em Layer 3; 4.2. O HA deve sincronizar: 4.2.1. Todas as sessões; 4.2.2. Certificados de-criptografados; 4.2.3. Todas Associações de Segurança das VPNs; 4.2.4. Todas as assinaturas de Anti-virus, Anti-spyware, Aplicações Web 2.0 e IPS; 4.3. O HA (modo de Alta-Disponibilidade) deve possibilitar tracking de IP. 4.4. Monitoração de falha de *link*. 4.5. Para melhor desempenho ou em caso de crescimento da rede, a solução deve suportar mais de dois membros no cluster de NG Firewall ou NGTP; 4.6. A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces; 4.7. Suportar agregação de links 802.3ad sem a limitação da combinação de portas devido hardware de aceleração proprietário do fabricante; 5. VPN 5.1. A solução deve suportar CA Interna e CA Externa de terceiros; 5.2. Solução deve suportar 3DES e AES-256 de criptografia para IKE Fase I e "Suite-B-MCG-128” “Suite-B-GCM-256" para a fase II; 5.3. Solução deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 e Grupo 20; 5.4. Solução deve suportar a integridade dos dados com MD5, SHA1, SHA-256, SHA-384 e AES-XCBC; 5.5. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web); 5.6. A Solução deve suportar clientless SSL VPN para acesso remoto; 5.7. Solução deve suportar VPNs baseadas em redes e VPNs através de rotas com suporte a protocolos de roteamento dinâmico; 5.8. Solução deve incluir a capacidade de estabelecer VPNs com gateways de IPs públicos dinâmicos; 5.9. Solução deve incluir compressão IP para client-to-site e VPN site-to-site; 5.10. Suportar IPSec VPN: 5.11. Criptografia DES, 3DES, AES128, AES256, AES-GCM-128 e AES-GCM-256; 5.12. Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC; 5.13. Diffie-Hellman Group 1, Group 2 e Group 5, Group 14, Group 19, Group 20; 5.14. Algoritmo Internet Key Exchange (IKE) versões I e II; 5.15. AES 128 ou 192 e 256 (Advanced Encryption Standard); 5.16. Permitir através da Gerência centralizada a criação e utiização de certificados gerados pela PKI interna da mesma que serão disponibilizado para acessos site-to-site e client-to-site; 5.17. Deve ser capaz de estabelecer VPN utilizando a funcionalidade Link Selection através do

protocolo Check Point RDP. Esta VPN será estabelecida com os equipamentos atualmente em uso na Justiça Eleitoral;

6. VPN SSL
   - 6.1. A solução deve suportar Secure Sockets Layer versão (SSL) 3, com os seguintes algoritmos de cifra simétrica e comprimentos de chave: RC4 (128 bits), 3DES (128 e 256bits) e AES (128 e 256bits);
   - 6.2. A solução deve possuir licenciamento para, no mínimo, 50 usuários simultâneos;
   - 6.3. A solução deve ter a opção de impor controle de login simultâneo, bloqueando sessões simultâneas do mesmo usuário;
   - 6.4. A solução deve possuir interface intuitiva, personalizável oferecendo aos usuários fácil acesso aos aplicativos, todos com um single-sign-on;
   - 6.5. Permitir suporte integrado à VPN SSL client-to-site nativo ou via licenciamento adequado;
   - 6.6. A VPN SSL deve oferecer um ambiente de trabalho seguro, criando um desktop virtual sobre o desktop normal dos usuários remotos, completamente isolado. Aplicações maliciosas e vírus presentes no desktop normal não podem afetar o desktop virtual. Todas as informações presentes do desktop virtual devem estar criptografadas;
   - 6.7. Além de criptografar e proteger informações de sessão do usuário, a solução de VPN SSL deve permitir ao administrador configurar quais aplicações podem ser executadas durante o uso do ambiente de trabalho seguro;
   - 6.8. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
   - 6.9. O cliente de VPN deverá estar disponível para as seguintes plataformas:
     - 6.9.1. Windows XP;
     - 6.9.2. Windows 7;
     - 6.9.3. Windows 8;
     - 6.9.4. Windows 10;
     - 6.9.5. iOS;
     - 6.9.6. Android;
     - 6.9.7. Mac OSX 10;
   - 6.10. Deverá suportar os seguintes navegadores:
     - 6.10.1. Internet Explorer 7 ou superior;
     - 6.10.2. Firefox 3.6 ou superior;
     - 6.10.3. Safari.

7. CONTROLE DE APLICAÇÕES WEB
   - 7.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB 2.0;
   - 7.2. A solução deve ser capaz de identificar qualquer tipo de aplicação Web 2.0 em até camada 7 independente de porta e protocolo;
   - 7.3. Possuir um reconhecimento de pelo menos 7100 aplicações diferentes, permitindo a consulta a base de aplicação em site público do fabricante, incluindo categorização para tráfego relacionado a aplicações peer-to-peer, redes sociais, acesso remoto, update de software, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
   - 7.4. Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, social widgets com controle granular para usuários ou grupos de usuários;
   - 7.5. A solução deverá prover controle de segurança granular de ao menos 250.000 Web 2.0 widgets
   - 7.6. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund);
   - 7.7. Deve possibilitar não apenas o bloqueio das aplicações, mas também de portas e protocolos. Deve ainda distinguir protocolos de aplicações, por exemplo o protocolo GRE não deve ser tratado como aplicação na política.
   - 7.8. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, onedrive, db2, mysql,

	oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs; 7.9. Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta padrão ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 389; 7.10. Solução deve ser capaz de criar regras com várias categorias. 7.11. Deve possibilitar a permissão ou bloqueio de aplicações por pelos menos os seguintes critérios: 7.11.1. Aplicação da Web; 7.11.2. Categorias; 7.11.3. Nível de risco; 7.11.4. IP/Range de IP's/Redes; 7.11.5. Usuários do AD/LDAP; 7.11.6. Diferentes grupos de usuários; 7.11.7. Aplicações que sejam passiveis a técnicas de evasão por *malwares* e uso excessivo de banda como (ultrasurf, torrent, dropbox e file sharing); 7.12. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD; 7.13. Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e gerência; 7.14. Devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários; 7.15. Deve suportar o controle de aplicações conhecidas e possibilitar a inclusão de aplicações desconhecidas localmente, ou, através de ticket direto com o fabricante. 7.16. Deve possibilitar a customização, por regra, da tela de interação com o usuário, permitindo: informar, questionar e limitar a banda de acesso; 7.17. Deve permitir diferentes "telas" de interação com o usuário para dispositivos móveis; 7.18. Deve possibilitar a diferenciação e controle granular específico das aplicações: Gmail, Gmail Enterprise, Gmail-Drive, Gmail-file-transfer, Gmail-file-transfer-download, Gmail-file-transfer-upload, Inbox-by-Gmail, Gmail-chat, Gmail-video-chat, Gmail-Voice-Chat, Gmail-Voice-Video-Chat, Gmail-call-phone, Viber, Viber-file-transfer, Viber-Voice-Call, Viber-Voice-message, WhatsApp-Messenger, WhatsApp-Messenger-file-transfer, WhatsApp-Messenger-Web, WhatsApp-Messenger-Voice-Call; 7.19. Deve permitir o bloqueio de aplicações Proxies: Ultrasurf, GPass, FreeGate, Hopster, Tor, HotSpot Shield 7.20. Deve permitir o bloqueio de aplicações: AirVPN, ClickTools, G-Cloud-Backup, Hide.Me, Intacct, JumboMail, JumboMail-Download, JumboMail-Upload, JumboMail-Share, Nearby, PubNub, Sfax, Zapier, pCloud, skyZIP, AeroFS, Rocket-League, Tresorit, okta, Alexa, HubSpot, PingOne e VPN-Shield; 7.21. Deve possibilitar a integração da solução com base do Active Directory, Ldap, Radius ou base local para criação de políticas. Possibilitando a criação de regras utilizando: 7.21.1. Usuários; 7.21.2. Grupo de usuários; 7.21.3. Máquinas (estações de trabalho); 7.21.4. Endereço IP; 7.21.5. Endereço de Rede; 7.21.6. Combinação das opções acima; 7.22. Possuir controle granular para quais funcionalidades de proteção, endereços IPs será executada a inspeção e de-criptografia de SSL tanto para tráfego de entrada (Inbound) e Saída (Outbound). 7.23. A Solução deve ter um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem para um período de tempo específico; 7.24. Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de

início e fim de validade);

7.25. Deve possibilitar a customização por regra utilizando as seguintes ações de controle:
- 7.25.1. Permitir;
- 7.25.2. Bloquear;
- 7.25.3. Monitorar;
- 7.25.4. Informar o usuário;

7.26. O mecanismo de Controle de aplicação deve apresentar contagem de utilização de regra de acordo com a utilização;
7.27. A solução deverá possuir uma interface de fácil utilização para buscas de Aplicações;
7.28. A solução deverá categorizar por Fator de Risco aplicações;
7.29. A solução deverá receber atualizações via internet para sua base;
7.30. A solução deverá possuir um mecanismo para informar ou perguntar ao usuário em tempo real com a finalidade de educá-los ou confirmar ações baseadas na política de acesso;
7.31. A solução deverá permitir a criação de exceções baseadas em objetos de rede;
7.32. A solução deve prover a opção de editar a notificação de bloqueio e redirecionar o usuário para a página de remediação;
7.33. A funcionalidade de Aplicação e filtros deverá possuir relatório de utilização.

8. IDENTIFICAÇÃO DE USUÁRIO
- 8.1. Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP e Radius;
- 8.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 8.3. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;
- 8.4. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- 8.5. Deve possuir suporte a identificação de múltiplos usuários conectados com um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular;
- 8.6. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- 8.7. Deve suportar autenticação para Smartphone e tablet’s;
- 8.8. Deve suportar autenticação Kerberos transparente para single sign on;
- 8.9. A solução deverá compartilhar e propagar a identificação de usuários com outros gateways de segurança do mesmo fabricante;
- 8.10. Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;
- 8.11. A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;
- 8.12. A solução de identificação de usuário deve suportar engine onde assume que um único usuário está conectado por computador;
- 8.13. A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;
- 8.14. A solução deve integrar-se perfeitamente com serviços de diretório, IF-MAP e Radius;
- 8.15. A solução deve permitir a identificação de usuários através de proxy via “X-forward headers”;
- 8.16. A solução deverá suportar grupos LDAP “nested”;

9. CONTROLE DE URL
- 9.1. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado ao Firewall NG;
- 9.2. A Solução deve ter um mecanismo configurável de bypass onde o administrador consegue

definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem de URL para um período de tempo específico;

9.3. Deve possuir as seguintes funcionalidades de filtro de URL:
9.4. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
9.5. Deve ser possível a criação de políticas por Usuários e Grupos de Usuários cadastradas no AD, Ips, Redes e Grupos de Redes.
9.6. A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
9.7. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização;
9.8. Deverá ser possível questionar o usuário e obrigar o mesmo a justificar na própria página a necessidade do acesso, permitindo assim o registro em logs passíveis de auditoria;
9.9. A solução de Filtro de URL deverá ser totalmente integrada com a solução de Aplicações WEB 2.0 para melhor gerenciamento e controle Next Generation;
9.10. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund), sendo que para a opção de OUTBOUND não será necessário efetuar o MITM, ou seja, a solução deverá prover algum mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso de acordo com a política configurada;
9.11. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
9.12. A solução deve possuir engine de bloqueio de conteudo em sites de busca como (Google, Bing e Yahoo). Assim como o bloqueio de sites que estão em modo cashed;
9.13. Deve possibilitar a customização por regra com as seguintes ações de controle:
9.13.1. Permitir;
9.13.2. Bloquear;
9.13.3. Monitorar;
9.13.4. Informar o usuário;
9.14. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no appliance (Captive Portal);
9.15. Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços.
9.16. Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs;
9.17. Deverá possuir pelo menos 60 categorias de URLs;
9.18. Deverá possibilitar a criação de Categorias de URLs customizadas;
9.19. Deverá possibilitar a exclusão de URLs do bloqueio por categoria;
9.20. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categoriza ou categorizada incorretamente;
9.21. Deve possibilitar a customização de pagina de bloqueio de interação com usuário;
9.22. Devem incluir informações das atividades dos usuários em seus logs;
9.23. Solução deve ter uma categorização URL que exceda 200 milhões de URLs;
9.24. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL.

10. PREVENÇÃO DE AMEAÇAS

10.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall sem a necessidade de uso de quaisquer interfaces externas onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança;
10.2. A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações;
10.3. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho sem degradar a performance do equipamento solicitado neste edital;
10.4. A solução de IPS deve fazer a inspeção de todo o trafego de forma bidirecional, analisando

	qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital; 10.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo; 10.6. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance; 10.7. Em cada proteção de segurança, deve estar incluso informações como: código CVE, tipo de impacto na ferramenta, severidade, e tipo de ação que a mesma irá executar; 10.8. A solução deve fazer captura de pacotes para proteções específicas; 10.9. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força a bruta a scanning de portas CIFS, Port overflow, Non Compliant SSL, IKE aggressive Exchange; 10.10. Deve ser capaz de bloquear tráfego SSH enviados em outras portas. 10.11. A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas; 10.12. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada; 10.13. As regras de exceção devem possuir: origem, destino e serviço; 10.14. A solução deve ser capaz de inspecionar tráfego HTTPS (inbound/Outbound); 10.15. Proteger o ambiente de ataque DoS; 10.16. Baseado nas melhores práticas de segurança e otimização de tempo operacional dos administradores, a solução de IPS integrada no appliance de segurança, deve possuir uma base de assinaturas de segurança superior a 5000 (cinco mil) assinaturas; 10.17. A solução de IPS deve possuir funcionalidade de simulação ou detecção do tráfego processado para fins de troubleshooting; 10.18. Na própria interface de gerência, a solução de IPS deve possuir índices por período (hora, semana ou mês) onde aponta o nível de ação das assinaturas baseada pela sua severidade; 10.19. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os appliances que estão sendo gerenciados informando no mínimo: Nome do Gateway, Endereços IP nas versões 4 e 6, Perfil Utilizado, Informação de status da funcionalidade de bypass e modo de operação (bloqueio ou detecção). 10.20. Para melhor administração da solução, a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente; 10.21. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção) das assinaturas recentemente baixadas via atualização sem alterar o padrão operacional do IPS previamente configurado; 10.22. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de mail, Web e DNS, onde as mesmas poderão ser assinaladas no momento da criação do objeto de rede na solução; 10.23. Deverá possibilitar a inclusão de novas assinaturas e customização no formato SNORT; 10.24. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance; 10.25. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino; 10.26. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, serviços Windows (Microsoft Networking) e VoIP; 10.27. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos; 10.28. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados

	10.29. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms; 10.30. A solução deve permitir a pré-configuração de, no mínimo, 15 perfis de proteção de IPS que podem ser utilizados a qualquer momento; 10.31. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo das opções granulares em: última hora, últimas 24 horas, última semana e último mês; 10.32. A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens ou destinos e combinações entre os dois; 10.33. A solução deve permitir a configuração de políticas baseada em países, dispondo de pelo menos 220 países já cadastrados em sua base; 10.34. A solução deve possuir os seguintes esquemas de Update de assinaturas: 10.34.1. Update instantâneo, através de um click; 10.34.2. Update através de agendamento onde engloba horário, dias da semana ou dia do mês; 10.34.3. Update de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução; 10.35. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP de entrada. Depois de importar esses certificados, a solução deve permitir o uso desses certificados na configuração de regra de IPS para Inspeção segura HTTP; 10.36. Dentro a engine de inspeção HTTPS, a solução deve permitir a criação de diferentes regras onde será especificado: origem, destino, tipo de serviço, ação e certificado que será atribuído por regra; 10.37. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos; 10.38. A solução deverá permitir a criação de perfil de proteção baseado em hosts internos ou servidores ou a combinação dos dois; 10.39. A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato; 10.40. A solução deverá possuir proteções para sistemas SCADA; 10.41. A solução deverá inspecionar o protocolo Citrix com a finalidade de comprovar que o tráfego é realmente o protocolo Citrix ICA; 10.42. Solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados; 10.43. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear. 10.44. Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança ou entregue em composição com outro fabricante desde que integrado à gerência centralizada de administração, monitoração e logs; 10.45. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas. 10.46. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego; 10.47. Implementar funcionalidade de detecção e bloqueio de callbacks; 10.48. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede; 10.49. A solução Antibot deve possuir mecanismo de detecção em multi-camadas que inclui, reputação de endereço IP, URLs e endereços DNS e detectar padrões de comunicação, assinaturas e análise de mensagens de email; 10.50. Implementar atualização da base de dados da rede de inteligência de forma automática, permitindo o agendamento diários e período (tempo) de cada atualização; 10.51. Implementar mecanismo de múltiplas fases para verificação de malware e/ou códigos maliciosos; 10.52. A solução deve analisar e bloquear malware e/ou codigos maliciosos pelo menos nos seguintes tipos de arquivos: bat, com, exe, dll, vsd, reg, jar, txt, swf, cmd, mpg, jse, midi, mp3, hlp, php, png, TIF, WAV, ASF, HTM, COM, JPEG; 10.53. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP e

	CIFS; 10.54. A solução deve atuar na prevenção de forma granular através de políticas por usuário / máquina ou Rede, sendo possível escolher um Profile diferente para cada regra; 10.55. A solução deve permitir criar regras de exceção de acordo com a proteção a partir do log visualizado na interface gráfica da gerencia centralizada; 10.56. Implementar através da interface gráfica de administração, configuração de mecanismo de alerta onde seja possível configurar bloqueio/desbloqueio de uma comunicação do tipo callback; 10.57. A solução deve ser capaz de bloquear uma conexão até que a classificação da mesma seja completada. 10.58. Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados; 10.59. A solução deve possuir na própria interface de gerencia, gráfico contento informações em tempo real sobre as atividades recentes de malwares detectados na solução, sendo que essas informações deverão ser apresentadas em mapa geográfico por país, através de IP ou URL e principais e-mails que foram scaneados; 10.60. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referente a incidentes de vírus e Bots; 10.61. A solução deve permitir de forma anônima compartilhar ou não informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do Fabricante; 10.62. A solução deve permitir a criação de White list baseado no MD5 do arquivo; 10.63. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.) 10.64. Em caso de falha no mecanismo de inspeção do anti-virus, deve ser possível configurar se as conexões serão permitidas ou bloqueadas; 10.65. A solução de anti-bot e anti-virus, deve possuir recurso onde o administrador consiga criar as regras de politica de segurança, permitindo salva-las e posteriormente aplicar para entrar em modo detect/inspect. 10.66. Caso o administrador tenha realizado alteração na solução de anti-virus ou bot, essa funcionalidade deve possuir opção de aplicação de regra apenas nesta engine, sem interferir nas demais regras de outras funcionalidades de segurança. Assim evitando confronto com alteração de outras funcionalidades; 10.67. A solução deve ser capaz de procurar por ações de BOTs. 10.68. A solução deve suportar a detecção e prevenção de vírus Cryptors & ransmoware; 10.69. A solução deverá possuir mecanismo para proteger contra ataques de Spear phishing; 10.70. Analisar padrões de comunicação C&C e não apenas o servidor DNS destino; 10.71. Funcionalidade DNS TRAP, que visa auxiliar na descoberta de hosts infectados que geram comunicação com C&C; 10.72. Capacidade para detectar e previnir ataque DNS tunneling; 10.73. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares; 10.74. A solução deve ser capaz de previnir acesso a websites maliciosos; 10.75. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos; 10.76. A solução deverá ser capaz de inspecionar arquivos comprimidos; 10.77. A solução antivirus deverá suportar a análise de links no corpo de e-mails; 10.78. A solução antivirus deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS; 10.79. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks; 10.80. Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS e TLS; 10.81. A solução deve possuir engine onde é possível determinar o tamanho de inspeção inicial de uma mensagem dentro do e-mail; 10.82. A solução deve possuir engine onde é possível determinar a inspeção da quantidade inicial de URL's dentro do e-mail; 10.83. A solução de prevenção de ameaças deve possuir engine onde seja possível não

	scanear endereço de e-mail de origem e destino e combinações dos dois; 10.84. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle; 10.85. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb; 10.86. A solução deve fornecer a capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, sendo eles: Windows XP e Windows 7 assim como office 2003, 2010 e 2013; 10.87. Conter ameaças de dia zero permitindo ao usuário final o recebimento do arquivo limpo e livre de malware além de permitir também, de acordo com a política de segurança, o download do arquivo original; 10.88. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas; 10.89. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego; 10.90. Implementar funcionalidade de detecção e bloqueio de callbacks (comunicação do malware com o servidor de comando e controle); 10.91. Implementar integração com ferramentas de SIEM; 10.92. Implementar mecanismo de integração com servidores syslog; 10.93. Conter ameaças avançadas de dia zero independente do sistema operacional; 10.94. A solução deve apresentar informações comportamental incluindo listagem de módulos e processos utilizados pelo malware e/ou código malicioso de forma sequencial; 10.95. Toda análise deverá ser realizada na nuvem, não sendo aceitas soluções que necessitem de módulos e/ou servidores de terceiros para a implementação de qualquer funcionalidade solicitada; 10.96. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador; 10.97. Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante; 10.98. A solução deve detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o fluxo de CPU; 10.99. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos; 10.100. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos; 10.101. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede, endereço IP; 10.102. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado. A solução deve suportar a inspeção de no mínimo os seguintes tipos de arquivo: CAB, CSV, DOC, DOCX, DOCM, DOT, DOTM, DOTX, EXE, HWP, JAR, PDF, PIF, PPAM, PPS, PPSM, PPSX, POTX, POTM, PPT, PPTM, PPTX, RAR, RTF, SCR, Seven-Z, SLDM, SLDX, SWF, TAR, TGZ, XLA, XLAM, XLL, XLW, XLS, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XLSB, ZIP; 10.103. A solução deve analisar e bloquear malware e/ou códigos maliciosos pelo menos os seguintes tipos de arquivos: 10.104. bat, com, exe.dll, vsd, reg, jar, txt, swf, cmd, mpg, jse, midi, mp3, hlp, php, png, TIF, WAV, ASF, HTM, COM, JPEG 10.105. A solução de anti-virus deve permitir o bloqueio de download de arquivos que excedam o tamanho pré-definido 10.106. A solução deve atuar na prevenção de forma granular através de políticas por usuário / máquina ou Rede, sendo possível escolher um profile diferente para cada regra; 10.107. A solução deve permitir criar regras de exceção de acordo com a proteção a partir do

	log visualizado na interface gráfica da gerencia centralizada; 10.108. Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de detecção e proteção, gráfico de top infecções, e gráfico da taxa de transferência de tráfego monitorado; 10.109. Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro; 10.110. Implementar mecanismo de pesquisa por diferentes intervalos de tempo; 10.111. Implementar através da interface gráfica, pesquisa aos eventos já reconhecidos; 10.112. A solução deve possuir mecanismo de controle onde seja possível configurar um indicador onde o administrador recebe um alerta em caso: 10.112.1. Tamanho máximo do arquivo emulado; 10.112.2. Tempo máximo de emulação; 10.113. Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados; 10.114. O sistema de emulação deve exibir percentual de arquivos scaneados; 10.115. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança; 10.116. Conter ameaças de dia zero que burlam o sistema operacional emulado; 10.117. A solução deve permitir de forma anônima compartilhar ou não informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do fabricante; 10.118. A solução deve permitir a criação de white list baseado no MD5 do arquivo; 10.119. A solução deve possuir engine onde bloqueia ou permite o trafego em caso de falha na inspeção do trafego até que a mesma seja classificada. 10.120. Caso o administrador tenha realizado alteração na solução de anti-malware, essa funcionalidade deve possuir opção de aplicação de regra apenas nesta engine, sem interferir nas demais regras de outras funcionalidades de segurança. 10.121. A solução deve possuir capacidade anti-evasão contra malware que tenta detectar a sua execução em uma SandBox; 10.122. Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso; 10.123. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração: 10.123.1. Quantidade de máquinas virtuais que estão atuando; 10.123.2. Número de arquivos emulados; 10.124. A funcionalidade de limpeza dos conteúdos ativos e exploits deve suportar os seguintes tipos de arquivos: DOC, DOCX, DOCM, DOT, DOTM, DOTX, FDF, PDF, PPAM, PPS, PPSM, PPSX, POTX, POTM, PPT, PPTM, PPTX, XLS, XLSX, XLTX, XLSM, XLTM, XLSB, XLAM; 10.125. A solução de appliance Sandbox, deve de possuir engine onde no momento que encontrado um conteúdo malicioso no arquivo office ou PDF, a mesma deve reconstruir o arquivo removendo o conteúdo malicioso, sendo capaz de converter arquivos reconstruídos para o formato PDF para melhor segurança, ou manter-se em formato original de acordo com política estabelecida. 10.126. A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias: 10.126.1. Arquivos scaneados; 10.126.2. Arquivos maliciosos; 10.127. A solução deve ser capaz de fazer atualizações de engines e até mesmo VM's em modo offline; 10.128. A solução deve monitorar atividades suspeitas em: 10.128.1. API calls; 10.128.2. File system changes; 10.128.3. System registry; 10.128.4. Network connections; 10.128.5. System processes; 10.128.6. File creation and deletion; 10.128.7. File modification;

10.128.8. Kernel code injection;
10.128.9. Kernel modifications;
10.128.10. Kernel code behavior (monitorando atividades de código em “non user-mode”);
10.128.11. Direct CPU interaction.
10.129. Emule atividades de interatividade como cliques de mouses e aberturas de arquivos;
10.130. Prover na gerência centralizada relatórios incluindo, no mínimo:
10.130.1. Telas que emulem ações dos usuários abrindo os arquivos através de cliques de mouses e aberturas de arquivos
10.130.2. Visões na linha do tempo;
10.130.3. Criações e Modificações de registro;
10.130.4. Criação de processos e arquivos;
10.130.5. Detecte atividades de rede.

11. CONSOLE DE GERÊNCIA E MONITORAÇÃO
11.1. A solução de gerência deverá ser separada do gateway de segurança onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto assim como logs e relatórios de forma unificada;
11.2. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;
11.3. A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS;
11.4. Implementar gerenciamento centralizado das licenças de utilização da solução, incluindo adição e remoção de licenças;
11.5. A solução de gerência centralizada deverá ser composta por uma console de gerenciamento;
11.6. A solução de gerencia centralizada deverá estar licenciada para o gerenciamento de todos os appliances fornecidos neste processo;
11.7. A solução deve proporcionar a opção de adicionar alta disponibilidade, utilizando um servidor em standby que é automaticamente sincronizado com o servidor primário;
11.8. Para melhor análise e administração do ambiente de segurança, a solução deve prover graficamente para cada regra, a informação da utilização da mesma através de “hit count”. Com no mínimo as seguintes informações:
11.9. Visualização do percentual de utilização em relação a outras regras;
11.10. Informar a primeira e última vez que a regra foi utilizada, de acordo com a política estabelecida;
11.11. Deve incluir a capacidade de confiar em CAs externas com a opção de verificar o certificado de cada gateway externo através de, no mínimo, DN e IP;
11.12. A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;
11.13. A gerência deve possuir console de Log onde deve ter a capacidade de visualizar os logs de segurança em tempo real permitindo ao administrador realizar as devidas análises para fins de troubleshooting;
11.14. A solução de gerência, deverá prover fácil administração na aplicação das políticas para os Gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, onde pode ser aplicada nos Gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho de configuração e aplicação de regra;
11.15. Deve possuir engine de visualização gráfica da topologia dos firewalls gerenciados, pela console centralizada;
11.16. Solução deve incluir o status de todos os túneis VPN, site-to-site e client-to-site sendo eles:
11.16.1. Túneis permanentes e seu estado de conexão;
11.16.2. Túneis;
11.17. A solução deverá prover informações gerais de cada gateway como volume de pacotes aceitos, conexões concorrentes, novas conexões e licenciamento informando o seu prazo de validade;

	11.18. A solução de monitoração deverá ser capaz de possuir filtro onde consegue monitorar todos os usuários remotos logados; 11.19. A filtragem de logs deve ser intuitiva, ou seja, através do fornecimento de uma palavra chave, idêntico a pesquisa do Google, é disponibilizado a visualização dos logs filtrados atualizados com qualquer semelhança a palavra chave digitada; 11.20. Solução deve ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, e registrar e alertar quando o túnel VPN está desconectado; 11.21. A solução dever ser capaz de criar filtro que permita a visualização de múltiplos logs como: 11.21.1. Top origem; 11.21.2. Top destino; 11.21.3. Principais acessos a determinados serviços; 11.21.4. Principais ações; 11.21.5. Principais funcionalidades de segurança utilizadas do Firewall; 11.21.6. Principais regras que foram utilizadas de acordo com o filtro criado; 11.21.7. Principais aplicações web utilizada de acordo com a funcionalidade de segurança disponível no Firewall; 11.22. Com o intuito de melhorar a rapidez na pesquisa de eventos e abrangência de período de busca do log, a solução ter a capacidade de possuir logs indexados; 11.23. Permitir o filtro de logs através da utilização de objetos existentes na base de regras do NGFW ao invés de digitar o endereço IP do host; 11.24. Permitir pesquisa de logs através de informações do código de protocolo IP e porta de origem; 11.25. Deve prover filtros pré-definidos de eventos com maior importância; 11.26. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows; 11.27. A solução de gerência centralizada deverá possuir capacidade de analisar logs e eventos com intuito de mitigar qualquer anomalia no ambiente independente do appliance de segurança estar sob ataque ou elevado consumo de CPU e memória; 11.28. Deve manter um canal de comunicação seguro, com criptografia baseada em certificados, entre todos os componentes que fazem parte da solução de segurança, gerência, gateways, armazenamento de logs e emissão de relatórios; 11.29. Possuir autoridade certificadora interna para geração de certificados; 11.30. A solução de logs da gerência dever ter a capacidade de criar múltiplos filtros customizados, sendo possível salvar em favoritos para visualizar em um momento posterior ou através de uma rotina constante; 11.31. Permitir nas regras de Firewall, Controle de Aplicação e URL a ação excessão para host e serviço; 11.32. A solução deve ser capaz de criar regras de exceção para determinado tipo de proteção a partir do log apresentado na solução; 11.33. O gerenciamento deve permitir: 11.33.1. Criação e administração de políticas de Firewall, Controle de aplicação e IPS; 11.33.2. Criação e administração de políticas de Antivírus e Anti-Malware; 11.33.3. Criação e administração de políticas de Filtro de URL e prevenção contra ameaças avançadas; 11.33.4. Criação e administração de políticas de VPNs IPSec e SSL; 11.33.5. Monitoração de logs; 11.33.6. Ferramentas de investigação de logs; 11.33.7. Debugging; 11.33.8. Captura de pacotes; 11.34. Acesso concorrente de administradores; 11.35. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores; 11.36. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos; 11.37. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

	11.38. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações; 11.39. Autenticação integrada à base de dados local ou servidor Radius; 11.40. Localização de em quais regras um endereço IP, Range de IP, subrede ou objetos estão sendo utilizados; 11.41. Deve atribuir sequencialmente um número a cada regra de Firewall, NAT e QoS; 11.42. Criação de regras que fiquem ativas em horário definido; 11.43. Criação de regras com data de expiração; 11.44. Backup das configurações e rollback de configuração para a última configuração salva; 11.45. Suportar Rollback de Sistema Operacional para a última versão local; 11.46. Habilidade de upgrade via SCP ou TFTP e interface de gerenciamento; 11.47. Validação de regras antes da aplicação; 11.48. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing); 11.49. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors); 11.50. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração; 11.51. Deve ser possível exportar os logs em CSV; 11.52. Rotação do log; 11.53. Exibição das seguintes informações, de forma histórica e em tempo real: 11.53.1. Situação do dispositivo e do cluster; 11.53.2. Principais aplicações; 11.53.3. Principais aplicações por risco; 11.53.4. Administradores autenticados na gerência da plataforma de segurança; 11.53.5. Número de sessões simultâneas; 11.53.6. Status das interfaces; 11.53.7. Uso de CPU; 11.54. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa; 11.55. Permitir a pesquisa na base de logs através de operadores boleanos e sintaxes "yesterday" e "today"; 11.56. Gerar alertas automáticos via: 11.56.1. Email; 11.56.2. SNMP; 11.56.3. Syslog; 11.57. Deverá ser compatível com a solução de proteção de rede e permitir o gerenciamento centralizado de diversos equipamentos; 11.58. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança; 11.59. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções; 11.60. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível/homologado com/para VMware ESXi; 11.61. Deve consolidar logs de todos os dispositivos administrados; 11.62. Deve permitir exportar backup de configuração automaticamente via agendamento; 11.63. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura; 11.64. Permitir que os logs de auditoria tenham identificação; 11.65. Permitir que todas as alterações em objetos gerem log de auditoria; 11.66. Permitir que todas as alterações das regras gerem log de auditoria; 11.67. Deve possuir mecanismo para identificar e informar aos administradores problemas de configuração de anti-spoofing;

11.68. Deve possuir mecanismo para checar e informar sobe uso de disco rígido, uso de memória, licenças, usuários e políticas da gerência centralizada;
11.69. A gerência centralizada deve prover no mínimo, em tempo real, a visualização estatística, gráfica linear e barras, das informações:
11.69.1. Visualização da quantidade de tráfego utilizado de aplicações e navegação;
11.69.2. Informações Gráficos;
11.69.3. Informações Estatísticas;
11.69.4. Interfaces mais utilizadas;
11.69.5. Serviços mais utilizados;
11.69.6. Destinos mais utilizados;
11.69.7. Volume de tráfego de entrada por regra;
11.69.8. Volume de tráfego de saída por regra;
11.69.9. Distribuição de pacotes em faixas de tamanho dos mesmos referenciado o volume e quantidade de pacotes por segundo;
11.69.10. Uso de CPU;
11.69.11. Número de conexões;
11.69.12. Taxa do número de pacotes por segundo aceitos;
11.69.13. Taxa do número de pacotes por segundo bloqueados;
11.69.14. Throughput;
11.69.15. Taxa de conexões por segundo;
11.69.16. Taxa de fragmentos processados por segundo;
11.69.17. Pico da taxa de pacotes por segundo decriptografados;
11.69.18. Taxa de pacotes por segundo decriptografados;
11.69.19. Pico da taxa de erros por segundo de decriptografia;
11.69.20. Taxa de erros por segundo de decriptografia;
11.69.21. Thoughput de decriptografia;
11.69.22. Pico da taxa de pacotes por segundo criptografados;
11.69.23. Taxa de pacotes por segundo criptografados;
11.69.24. Pico da taxa de erros por segundo de criptografia;
11.69.25. Taxa de erros por segundo de criptografia;
11.69.26. Thoughput de criptografia;

12. MÓDULO DE RELATÓRIOS E CORRELAÇÃO DE EVENTOS
12.1. Permitir a análise através de relatório da utilização de aplicações entre período histórico e presente;
12.2. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus, AntiMalware e Emulação), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
12.3. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e AntiMalware);
12.4. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, AntiMalware e Emulação), e URLs que passaram pela solução;
12.5. Gerar relatórios, contemplando no mínimo:
12.5.1. Resumo gráfico de aplicações utilizadas;
12.5.2. Principais aplicações por utilização de largura de banda;
12.5.3. Principais aplicações por taxa de transferência de bytes;
12.5.4. Principais hosts por número de ameaças identificadas;
12.5.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e AntiMalware), de rede vinculadas a este tráfego;
12.5.6. Deve permitir a criação de relatórios personalizados;
12.6. Disponibilizar relatório gráfico do percentual de eventos por CVE (Common Vulnerabilities and Exposures);
12.7. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução;
12.8. Deverá possuir mecanismo "Drill-Down" para navegação e análise dos logs em tempo real;

	12.9. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso; 12.10. Deve incluir uma ferramenta do próprio fabricante ou solução de terceiros para correlacionar os eventos de segurança das funcionalidades adquiridas neste edital, sendo ele capaz de receber eventos de soluções de mercado; 12.11. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino; 12.12. Disponibilizar informações gráficas, na linha tempo que informe o número de eventos ocorridos; 12.13. Disponibilizar recursos interativos de navegação nos eventos informados; 12.14. Correlacionar eventos capaz de utilizar como base informações o número de conexões em determinado tempo seguido pelo menos das ações: bloqueio da origem, envio de SNMP e envio de e-mail; 12.15. A solução deve exportar relatórios via HTML, CSV e MHT; 12.16. A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados; 12.17. A solução deve permitir ao administrador atribuir filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador o foco sobre os eventos mais importantes; 12.18. A solução deve prover no mínimo as seguintes funcionalidades para análise avançada dos incidentes: 12.18.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação; 12.18.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada; 12.18.3. Estatísticas com comparativo de período (hora, dia e mês); 12.19. Deve permitir a geração de relatórios com horários pré definidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos; 12.20. Deve mostrar a distribuição dos diferentes eventos filtrados por país em um mapa, onde deve estar incluso principais eventos de origem ou destino por país; 12.21. Deve permitir ao administrador o agrupamento de eventos baseado em quaisquer características, incluindo vários níveis de alinhamento; 12.22. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares; 12.23. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias; 12.24. Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes; 12.25. Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado; 12.26. Deve suportar a geração de relatório gráfico gerencial, provendo o consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos além do consumo interno dos usuários; 12.27. A solução dever ser capaz de criar ticket interno para maior mitigação de eventos, sendo possível editar comentários pelo administrador no momento da mitigação do evento; 12.28. Deve implementar, ou utilizar solução de terceiros, no mínimo, os seguintes tipos de correlação de eventos: 12.28.1. Compressão: Consiste em reduzir múltiplas ocorrências de um mesmo evento por um único evento, indicando quantas vezes o evento ocorreu durante o período de observação; 12.28.2. Filtragem: Consiste em suprimir um determinado evento, em função dos valores de um conjunto de parâmetros, previamente especificados; 12.28.3. Contagem: Capacidade de quantificar/contar a ocorrência de um mesmo evento; 12.28.4. Escalação: É a capacidade de um evento, através da análise de outros eventos ser considerado de maior importância ou severidade;

12.28.5. Permitir a partir da console administrativa, selecionar o appliance e iniciar a requisição de suporte do fabricante.

13. MÓDULO DE *COMPLIANCE*
    - 13.1. A solução proposta deve mostrar através da interface gráfica quais gateways estão em conformidade com as normas PCI DSS 2.0, PCI DSS 3.0, ISO27001, ISO27002 e SOX;
    - 13.2. A solução deve simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;
    - 13.3. A solução deve permtir a customização do padrão regulatório da própria instituição;
    - 13.4. A solução deve pemitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;
    - 13.5. A solução deve monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;
    - 13.6. Deve ser possível gerar um relatório atual das políticas e configurações implementadas na console gráfica, e este ser enviado por e-mail ou salvá-lo em pdf;
    - 13.7. A solução deve alertar caso o *gateway* monitorado não esteja configurado para que o relógio seja sincronizado com NTP;
    - 13.8. A solução deve apontar caso na política de controle de acesso WEB não esteja configurado para bloquear sites de sexo, jogos, nudez, pornografia;
    - 13.9. A solução deve impedir brechas de segurança por má configuração das regras, para isso, deve permitir ao administrador configurar suas próprias regras de melhores práticas. Ex.: Definir que nenhuma regra pode ficar com o comentário em branco. Ex. 2: Não permitir tráfego FTP dos servidores da DMZ para a Rede Interna;
    - 13.10. A solução deve alertar em tempo real caso o Administrador crie uma regra com origem "Any" na política de segurança;
    - 13.11. A solução deve alertar em tempo real caso o Administrador crie uma regra com destino "Any" na política de segurança;
    - 13.12. A solução deve apontar as regras que não tiveram os contadores incrementados nos últimos 3 meses para que essas sejam removidas da política;
    - 13.13. Deve ser possível listar quais são as melhores práticas configuradas por grupos: tipo do grupo, status e funcionalidade;
    - 13.14. Cada verificação deve possuir uma descrição que identifique qual ação é executada e listar em quais normas faz parte dos requisitos;
    - 13.15. A solução deve vir pré-configurada com melhores práticas para regras de: Proteção contra Bots, Anti-Spam, Anti-vírus, Controle de Aplicação, Prevenção de vazamento de informações, Firewall, Sistema Operacional do Gateway de Segurança, Identificação de usuários, IPS, VPN Site-to-Site, VPN Client-to-Site, Emulação de arquivos e Controle de navegação Web;
    - 13.16. A solução deve verificar se a inspeção SSL está habilitada quando configurado as proteções de filtro de URL, controle de aplicação e IPS.

14. SERVIÇO DE INSTALAÇÃO
    - 14.1. Compreende-se nesta etapa a instalação de equipamentos, sistemas, softwares e aplicativos da CONTRATANTE nos PRODUTOS fornecidos, bem como a migração das configurações existentes na CONTRATANTE para os PRODUTOS fornecidos pela CONTRATADA;
    - 14.2. A migração das regras de segurança deverá ser realizadas de forma automatizada, com uso de software/script desenvolvido especificamente para este fim, com vistas a minimizar o impacto de um possível erro humano nas migrações de configurações;
    - 14.3. Caberá a CONTRATANTE o acompanhamento da migração, fornecimento de informações sobre os aplicativos e ferramentas existentes no ambiente, bem como a definição e concessão de janelas de intervenção;
    - 14.4. A etapa de implantação e migração deve acontecer de forma gradual e transparente, de acordo com a conveniência da CONTRATANTE;
    - 14.5. Durante a etapa de implantação e migração, os PRODUTOS fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção;

14.6. Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de implantação e migração definidos pela CONTRATANTE;
14.7. As atividades de implantação e migração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana;
14.8. A CONTRATADA deve garantir que a migração não irá alterar as versões ou o funcionamento dos serviços instalados na unidade objeto da migração, sem a prévia autorização da CONTRATANTE;
14.9. A CONTRATADA deverá, com a supervisão da CONTRATANTE, planejar e realizar a instalação dos softwares e a configuração dos novos equipamentos com total interoperabilidade operacional com ambiente atual da CONTRATANTE, sem impacto no ambiente de produção;
14.10. Durante a implantação e integração, a CONTRATADA deverá realizar, entre outras atividades: instalação de *softwares*, acompanhamento de migrações de regras e políticas, elaboração e execução de *scripts*, análise de desempenho, *tunning*, resolução de problemas e implementação de segurança;
14.11. Para implantação e migração devem ser consideradas as seguintes premissas:
14.11.1. Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como *hardwares*, *softwares*, recursos humanos necessários à instalação dos PRODUTOS.
14.11.2. A CONTRATANTE realizará transferência de conexão dos equipamentos conectados à rede LAN existente na CONTRATANTE para os PRODUTOS fornecidos;
14.11.3. A CONTRATADA realizará adequação/configuração dos PRODUTOS fornecidos ao longo da etapa de migração e realização de novas configurações;
14.12. A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação/migração e ao pleno funcionamento do ambiente de produção.

15. SERVIÇO DE SUPORTE TÉCNICO ON-SITE
15.1. O atendimento para hardware será do tipo “on-site” mediante manutenção corretiva nas dependências do TRE-BA, realizado por profissionais certificados e deverá cobrir todo e qualquer defeito apresentado, incluindo a substituição de peças, componentes, ajustes, reparos e correções necessárias;
15.2. O atendimento deverá acontecer 24 (vinte e quatro) horas por dia e sete dias por semana;
15.3. O tempo para o atendimento inicial do chamado de hardware será de 2 (duas) horas, após a abertura do chamado, e o prazo máximo para solução deverá ser de 15 (quinze) dias após a abertura do chamado;
15.4. O atendimento deverá incluir troca de peças ou componentes mecânicos ou eletrônicos, sem que isso implique em ônus adicional para o TRE-BA além daquele já cotado na proposta;
15.5. A substituição de peças e/ou componentes mecânicos ou eletrônicos de marcas e/ou modelos diferentes dos originais cotados pela CONTRATADA, somente poderá ser efetuada mediante análise e autorização do TRE-BA;
15.6. Todas as peças e componentes mecânicos ou eletrônicos substituídos deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos utilizados na fabricação do(s) equipamento(s), sendo sempre “novos e de primeiro uso”;
15.7. O atendimento para os softwares será do tipo telefônico, 24 (vinte e quatro) horas por dia e sete dias por semana. Deverá ser realizado por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado;
15.8. O tempo para o atendimento inicial de suporte a software do chamado de software será de 2 (duas) horas, após a abertura do chamado, e o prazo máximo para solução deverá ser de 30 (trinta) dias corridos, contados da abertura do chamado, desde que a falha não comprometa o funcionamento da solução.

16. GARANTIA
16.1. **A garantia do equipamento deverá ser de 36 meses**.

7	**LICENÇA PARA SOLUÇÃO UNIFICADA DE SEGURANÇA DA SEDE** **Marca: SonicWALL. Modelo: 01-SSC-4236 - COMPREHENSIVE GATEWAY SECURITY SUITE FOR NSA 5600 (3 YR).** 1. CARACTERÍSTICAS GERAIS Licença CGSS para *cluster* SonicWALL NSA 5600, por 36 meses.
8	**LICENÇA PARA SOLUÇÃO UNIFICADA PARA CARTÓRIO** **Marca: SonicWALL. Modelo: 01-SSC-4838 – COMPREHENSIVE GATEWAY SECURITY SUITE BUNDLE FOR TZ 205 SERIES (1 YEAR).** 1. CARACTERÍSTICAS GERAIS Licença CGSS para equipamento SonicWALL TZ 205W, por 12 meses.