	TERMO DE REFERÊNCIA	FOR-DILOG-001-09 (v.01)

1. OBJETO:

1.1. Contratação de Empresa especializada para a prestação de serviços de conectividade utilizando IP/MPLS ou VPN SDWAN, com recurso de segurança e wifi em cada perímetro de rede instalado, ferramentas e serviço para análise e mitigação de vulnerabilidades WEB e Link Seguro de acesso à rede mundial de computadores (Internet) com operadoras distintas, interligando as redes locais dos Fóruns das Comarcas do interior do Estado do Acre aos prédios do Tribunal de Justiça localizados na cidade de Rio Branco, por um período de 12 (doze) meses, conforme disposições deste Termo de Referência.

1.2. Esta rede deverá prover a comunicação centralizada de dados do Tribunal de Justiça, e os: Fóruns, Anexos Administrativos, Comarcas do Interior, também deverá prover o acesso à rede mundial de computadores - Internet. Os serviços deverão incluir fornecimento de hardware (modems e roteadores), solução de segurança e wifi gerenciada centralizada, solução de segurança de aplicações, software de gerenciamento, infraestrutura adicional e enlaces de comunicação com base na tecnologia Multiprotocol Label Switching – MPLS ou VPN IP SD-WAN, implantação, operação e manutenção destes enlaces, conforme especificações contidas neste Termo de Referência.

2. DETALHAMENTO DO OBJETO:

2.1. A Empresa CONTRATADA deverá fornecer Links Urbanos e Interurbanos para interligação da sede do Poder Judiciário do Estado do Acre, Localizado na Rua Tribunal de Justiça s/n, Via Verde, CEP: 69.920-193, Anexo “A” – DITEC, utilizando tecnologia MPLS ou semelhante superior com disposições e características, com as especificações abaixo:

2.1.1. Links com acesso à Internet com banda igual 500 Mbits (quinhentos Mbits) e 300 Mbits (trezentos Mbits) ou superior, em Fibra Óptica com tecnologia SDH, Ethernet/Metro, GPON ou outras tecnologias compatíveis, suportando o protocolo TCP/IP, com 100% de garantia de utilização de banda e obedecendo aos seguintes parâmetros:

GRUPO 1 - SERVIÇO DE CONECTIVIDADE, COMUNICAÇÃO E SEGURANÇA DA INFORMAÇÃO

ITEM		**ESPECIFICAÇÃO**					**QUANT**
		DESCRIÇÃO	VELOCIDADE	CPE SEGURANÇA	CPE WIFI	QTD CPE WIFI	
Serviço de acesso dedicado à Internet	01	Serviço de acesso dedicado à Internet com proteção em backbone contra ataques DDoS, Solução integrada de segurança de perímetro através do tipo UTM/NGFW Gerenciamento Centralizado e Armazenamento de log, funcionalidades SD-WAN e Serviço de Monitoramento proativo para o Anexo “A” da Sede do Tribunal de Justiça (DITEC).	500 Mbps	TIPO 1	N/A	N/A	01

Serviço de conectividade IP/MPLS ou VPN SDWAN contemplando serviço de monitoramento proativo, com Solução integrada de segurança do tipo NGFW com funcionalidades de SD-WAN e gerenciamento centralizado, solução de gerenciamento e distribuição da rede sem fio (controladora e pontos de acesso) tipo “indoor”.	02	Concentrador - Rio Branco	400 Mbps	N/A	TIPO 1	N/A	01
	03	Link Interurbano Fórum de Senador Guiomard. Avenida Castelo Branco, S/N – CEP 69.925-000. Senador Guiomard.	20 Mbps	TIPO 3	TIPO 1	3	01
	04	Link Interurbano de 20 Mbps: Fórum de Plácido de Castro. Rua Juvenal Antunes, 1079 – CEP 69.928-000. Plácido de Castro.	20 Mbps	TIPO 3	TIPO 1	3	01
	05	Link Interurbano de 20 Mbps: Fórum de Acrelândia. Av. Governador Edmundo Pinto, 581 – CEP 69.945-000. Acrelândia.	20 Mbps	TIPO 3	TIPO 1	3	01
	06	Link Interurbano de 20 Mbps: Fórum de Capixaba. Rua Francisco Cordeiro de Andrade, S/N – CEP 69.922-000. Capixaba.	20 Mbps	TIPO 3	TIPO 1	3	01
	07	Link Interurbano de 20 Mbps: Fórum de Xapuri. Rua Floriano Peixoto, 62 – CEP 69.930-000. Xapuri.	20 Mbps	TIPO 3	TIPO 1	3	01
	08	Link Interurbano de 20 Mbps: Fórum de Sena Madureira. Rua Cunha Vasconcelos, 689 – CEP 69.940-000. Sena Madureira.	20 Mbps	TIPO 3	TIPO 1	3	01
	09	Link Interurbano de 20 Mbps: Fórum de Manoel Urbano. Rua Mendes de Araujo, 1.267 – CEP 69.950-000. Manoel Urbano.	20 Mbps	TIPO 3	TIPO 1	3	01
	10	Link Interurbano de 20 Mbps: Fórum de Feijó. Travessa Floriano Peixoto, 206 – CEP 69.960-000. Feijó.	20 Mbps	TIPO 3	TIPO 1	3	01
	11	Link Interurbano de 20 Mbps: Fórum de Tarauacá. Avenida Antônio Frota, S/N – CEP 69.970-000. Tarauacá.	20 Mbps	TIPO 3	TIPO 1	3	01
	12	Link Interurbano de 50 Mbps: Cidade da Justiça de Cruzeiro do Sul. BR 307, KM 09, nº 4090 – CEP 69.980-000. Cruzeiro do Sul.	50 Mbps	TIPO 2	TIPO 1	3	01
	13	Link Interurbano de 20 Mbps: Fórum de Mâncio Lima. Rua Joaquim G. de Oliveira, 160 – CEP 69.990-000. Mâncio Lima.	20 Mbps	TIPO 3	TIPO 1	3	01
	14	Link Interurbano de 20 Mbps: Fórum de Brasiléia. AV. Geny Assis, S/N – CEP 69.932-000. Brasiléia.	20 Mbps	TIPO 3	TIPO 1	3	01
	15	Link Interurbano de 20 Mbps: Fórum de Epitaciolândia. BR 317, KM 01 – CEP 69.934-000. Epitaciolândia.	20 Mbps	TIPO 3	TIPO 1	3	01
	16	Link Interurbano de 20 Mbps: Fórum de Assis Brasil. Rua Dom Giocondo Maria Grotti, 281 – CEP 69.935-000. Assis Brasil.	20 Mbps	TIPO 3	TIPO 1	3	01
	17	Link Interurbano de 20 Mbps: CIC – Centro Integrado de Cidadania. Rua do Comércio, S/N – CEP 69.921-000. Porto Acre	20 Mbps	TIPO 3	TIPO 1	3	01
	18	Link Interurbano de 20 Mbps: CIC – Centro Integrado de Cidadania. Avenida Presidente Vargas, S/N – CEP: 69.985-000. Rodrigues Alves.	20 Mbps	TIPO 3	TIPO 1	3	01
	19	Link Urbano de 20 Mbps: Fórum de Bujari. BR 364, KM 28, Nº 390, Bujarí - Acre – CEP 69.923-000	20 Mbps	TIPO 3	TIPO 1	3	01
Serviço de solução web application	20	Serviço de solução web application firewall (WAF) e reconhecimento, análise e classificação de vulnerabilidades web capaz de prover proteção aos servidores de aplicação web na sede DITEC.	N/A	N/A	N/A	1	N/A

GRUPO 2 - SERVIÇO DE CONECTIVIDADE COM LINK DE INTERNET URBANO SECUNDÁRIO PARA REDUNDÂNCIA			
ITEM	**ESPECIFICAÇÃO**		**QUANTIDADE**
	DESCRIÇÃO	VELOCIDADE	
21	Serviço de acesso dedicado à Internet com proteção em backbone contra ataques DDoS e serviço de monitoramento proativo para redundância e dupla abordagem de saída de Internet para uso de funcionalidades de SD-WAN.	300 Mbps	01
22	Solução de proteção em backbone contra ataques DDoS.	N/A	01

a) A Empresa contratada do GRUPO 1, não poderá ser a Empresa contratada do GRUPO 2 e vice-versa.

b) A condição descrita no item acima, se deve a necessidade de criar uma contingência entre os Links de Internet, ou seja, somente em catástrofes naturais extremas ou casos fortuitos o acesso à rede Mundial de Computadores Internet será interrompido.

c) Link dedicado com estrutura exclusivamente em fibra óptica até seu ponto final.

d) Não serão aceitos links dedicados via enlace de rádio digital, ou par metálico, mesmo que devidamente licenciado e autorizado pela Anatel.

e) Fornecimento de conectividade IP – Internet Protocol – a 500 Mbits (velocidade fixa, full duplex, síncrona, simétrica e permanente) e 300 Mbits (velocidade fixa, full duplex, síncrona, simétrica e permanente), respectivamente para ITEM 01 do GRUPO 1 e ITEM 01 do GRUPO 2, que suporte aplicações TCP/IP e proveja o acesso à rede Internet.

f) O acesso deverá ser permanente (24 horas por dia e 07 dias por semana, a partir de sua ativação), dedicado, exclusivo, ou seja, serviço determinístico na rede de acesso e com total conectividade IP.

g) Todo o serviço de Internet deverá ser disponibilizado por meio de conexão direta e exclusiva da CONTRATANTE a um provedor de backbone Internet, não sendo necessária a contratação de provedor de acesso por parte da CONTRATANTE.

h) Fornecimento de, no mínimo, 254 (duzentos e cinquenta e quatro) números IPs próprios/públicos e válidos na Internet para o ITEM 01 do GRUPO 1 e de, no mínimo, 254 (duzentos e cinquenta e quatro) números IPs próprios/públicos e válidos na Internet para o ITEM 01 do GRUPO 2.

i) O índice de latência, perda de pacotes e disponibilidade do serviço deverão atender aos valores expressos abaixo:

- Latência (milissegundos): consiste no tempo médio de trânsito (ida e volta – roundtrip) de um pacote de 64 bytes entre dois pontos de backbone. É usada a média do backbone considerando o centro de gerenciamento da rede e cada um dos centros de roteamento. Objetivo: 120 ms.
- Perda de Pacotes (%): consiste na taxa de falha na transmissão de pacotes IP entre dois pontos do backbone. É usada a média do backbone considerando o centro de gerenciamento da rede e cada um dos centros de roteamento. Objetivo: 2,0%.
- Disponibilidade (%): consiste no percentual de tempo no qual a rede está operacional em um período de tempo. É considerado o ROTEADOR DE ACESSO (do Backbone) no qual está instalada a porta de conectividade IP do cliente. Objetivo: 99,0%.

j) O equipamento roteador deverá ser fornecido pela empresa e acoplável a Rack de 19'', atendendo às seguintes especificações:

- Possuir, no mínimo, 01 (uma) porta óptica de acordo com os Standarts ITU-G.984 GPON.
- Possuir, no mínimo, 04 (quatro) Gigabit Ethernet 10/100/1000 de detecção automática que sejam compatíveis com os padrões ISSO 8802.3 e IEE 802.3.
- A interface física da porta LAN deverá ser fornecida no padrão RJ-45 (10baseT), para cabos UTP, CAT 6 ou AUI.
- Possuir opção de boot local via memória flash ou similar.
- Permitir ser alimentado de forma automática por tensões de 110/220 VAC, frequência 60 Hz com duas fontes redundantes.
- Deverá suportar e implementar serviços de DHCP Server.
- Deverá ser gerenciável via SNMP.

2.1.2. Pontos de Interligação Interurbana (Links Interurbanos), à sede do Poder Judiciário do Estado do Acre, na sala de Servidores da Diretoria de Tecnologia da Informação – DITEC/TJAC, em Rio Branco - Acre:

2.2. As empresas contratadas dos GRUPO 1 e GRUPO 2 – Links de Internet Urbano e Interurbano, deverão obrigatoriamente instalar e manter, na Sede do Poder Judiciário do Estado do Acre, localizado Rua Tribunal de Justiça, s/n, Via Verde, Anexo A – DITEC, um Link com acesso à Internet com banda igual ou superior a 500 Mbits (quinhentos Mbits) e um Link com acesso à Internet com banda igual ou superior a 300 Mbits (trezentos Mbits), respectivamente ITEM 01 do GRUPO 1 e ITEM 01 do GRUPO 2, com tecnologia SDH, Ethernet/Metro Ethernet, GPON ou outras tecnologias, suportando o protocolo TCP/IP, com 100% de garantia de utilização de banda e obedecendo aos parâmetros do item 2.1.1

2.3. Inclui-se, na execução dos serviços a ser contratado, o fornecimento de equipamentos necessários ao funcionamento dos serviços objeto deste Termo de Referência, bem como a instalação, garantia de peças, suporte e assistência técnica permanente ao equipamento, objetivando atender nossa necessidade atual de comunicação, com manutenção e reposição de partes e peças desgastadas pelo uso normal do equipamento. A solução proposta deverá contemplar todos os equipamentos necessários, tais como: modem, roteadores, Sub-bastidor, fontes, softwares, numeração IP válida e serviços necessários para implantação e manutenção dos mesmos. O valor, tanto de instalação, quanto mensal do Link de Internet, bem como roteador e equipamentos necessários, deverão estar previstos na formação de preço dos itens.

2.4. As Licitantes a serem CONTRATADAS aplicarão nos equipamentos, quando necessário, a substituição de partes e peças originais, adequadas, novas ou, quando não, que mantenham as especificações técnicas do fabricante, ficando desde logo, autorizada pelo PODER JUDICIÁRIO DO ESTADO DO ACRE.

2.5. Os endereços das unidades do TJAC previstas para serem interligadas, estão relacionados aos GRUPO 1 e GRUPO 2 com os endereços, bandas e classes constantes neste Anexo foram levantados no momento da elaboração deste Termo de Referência, e podem ser alterados. No decorrer da vigência do contrato de prestação de serviço poderá eventualmente haver mudança de endereços, bandas e classes das unidades da TJAC, assim como a adição de novas unidades no projeto. No caso de mudança de endereços e a adição de novas unidades, a CONTRATADA deverá arcar com os respectivos custos de alteração da rede, desde que não seja necessário o desenvolvimento de projetos especiais para atendimento, estimulado por estar fora da área de ATB, definido pela ANATEL, ou que não seja um concentrador instalado em Fibra Ótica.

2.6. Havendo a necessidade de desenvolvimento de projetos especiais para mudança de endereço e/ou adição de novas unidades, a CONTRATADA deverá apresentar uma planilha de valores referente à alteração/adição, para previa aprovação da CONTRATANTE.

2.7. A empresa contratada para o(s) item(ns), independentemente da quantidade, deverá obrigatoriamente instalar acesso terrestre sobre fibra óptica para os Concentradores de Rede e manter, sem ônus a CONTRATANTE, na Diretoria de Tecnologia da Informação do Poder Judiciário do Estado do Acre, localizado Rua Tribunal de Justiça, s/n, Via Verde, ANEXO A – DITEC, um Link com banda igual à somatória de todas as bandas do concentrador do ITEM 2 do GRUPO 1, garantindo 100% de banda, conforme descrição acima.

2.8. Requisitos Obrigatórios para os Links Urbanos e Interurbanos:

ITEM	REFERÊNCIA	URBANO	INTERURBANO
Tipo de Acesso	Acesso por Fibra Óptica, que garantam o funcionamento de todas as especificações deste Termo de Referência.	Sim	Sim
Disponibilidade de Serviço	Relação entre o tempo de operação plena e prejudicada no período de 30 dias.	99%	98%

Tempo Máximo de Retardo Admissível	O tempo máximo de retardo na comunicação unilateral entre o ponto de conexão e o roteador de borda da Proponente para um pacote de 32 bytes.	Fibra Óptica: = ou < 120 MS	Fibra Óptica: = ou < 90 MS	
			Demais Conexões: = ou < 120 MS	
Banda Mínima Garantida	Banda mínima disponível para acesso à Internet para cada um dos pontos contemplados.	Fibra Óptica: 100% da banda	Fibra Óptica: 100% da banda	
			Demais Conexões: 50% da banda	
Ativação	Período entre a solicitação e ativação do Serviço.	Até 60 (sessenta) dias	Até 60 (sessenta) dias	
Prazo de Manutenção	Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento.	12 (doze) horas	24 (vinte e quatro) horas	
Prazo Mínimo de notificação de Manutenção Preventiva ou Atualização de Recursos Técnicos	Período mínimo entre a notificação do cliente pela operadora até o início da interrupção programada.	07 (sete) dias	07 (sete) dias	
Abertura de Chamado	Disponibilidade de atendimento para solicitações de reparos, *HELPDESK* da Operadora CONTRATADA e discagem sem cobrança (0800) em língua portuguesa.	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	
Horário de Reparo	Disponibilidade de atendimento técnico a partir da abertura da chamada.	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	
	Casos de responsabilidade da CONTRATADA: (Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento.).	Em Rio Branco: Máximo de 03 (três) horas.	Até 300 km de Rio Branco: Máximo de 06 (seis) horas	Acima de 300 km de Rio Branco: Máximo de 12 (doze) horas

2.9. A(s) empresa(s) contatada(s) do(s) item(s) acima relacionados deverá fornecer os seguintes concentradores:

GRUPO	CONCENTRADOR DE REDE ITEM 02 GRUPO 2	ENDEREÇO	TIPO
01	Sede do Poder Judiciário do Estado do Acre.	Rua Tribunal de Justiça, s/n, Via Verde, Anexo I – DITEC.	Urbano

3. JUSTIFICATIVA:

3.1. DA MOTIVAÇÃO:

3.1.1. O presente Termo de Referência tem por finalidade a contratação de empresa ou consórcio de Empresas de Telecomunicações para a prestação de serviços de comunicação de dados, utilizando protocolo IP MPLS ou VPN IP SD-WAN, para formar a rede WAN do Tribunal de Justiça do Estado do Acre, bem como a execução de conexões entre os diversos pontos e a interligação desta rede interna com a Internet, conforme detalhado no presente Termo de Referência, onde deverão ser disponibilizados os equipamentos necessários (modems, roteadores) para estes serviços, em conformidade com as especificações constantes neste instrumento. A rede ofertada deverá ter como ponto concentrador a cidade de Rio Branco, de onde sairão conexões para todas as localidades mencionadas na tabela de acessos. Esta topologia possibilita um melhor gerenciamento, pois a rede contemplará um único ponto central.

3.1.2. Esses links interligam todos os Fóruns do Estado do Acre ao edifício sede do Tribunal de Justiça. Atualmente os mesmos encontram-se sobrecarregados em virtudes dos serviços prestados tanto internamente como à comunidade. Muitos desses serviços foram acrescentados diretamente à rede do Tribunal. Abaixo citamos alguns serviços prioritários que dependem de links estáveis e rápidos:

a) Diário da Justiça: Todos os documentos que são publicados no diário da justiça são enviados pelos cartórios de todas as Comarcas do estado e também pelos Departamentos do Tribunal de Justiça via rede utilizando este link de comunicação. Isto é feito durante todo o dia, até as 16:00 horas. Esta transferência realiza-se em duas fases: O cartório envia a matéria para o servidor de arquivos e o setor gráfico transfere deste servidor para os usuários responsáveis pela formatação do diário.

b) Internet e Intranet: O acesso à Internet e a Intranet ficam prejudicados pelos dados que trafegam na rede. Quando os usuários acessam os sistemas da Intranet (Diário da Justiça, Help Desk, Jurisprudência, Consulta Processual, dentre outros).

c) Todos os processos Judiciais que tramitam no âmbito do Tribunal de Justiça são totalmente virtuais. Consequentemente as maiores unidades e Comarcas necessitam de links maiores.

3.1.3. Se o Tribunal quer continuar entre os primeiros, há a necessidade de que a comunicação, a segurança da informação, a disponibilidade e acessibilidade sejam prioridades e de grande relevância, com largura de banda suficiente para que os serviços operem de maneira satisfatória para seus funcionários e para a população em geral.

O objeto da presente licitação foi agrupado pelos GRUPOS, à luz do art. 23, §1º da Lei Geral de Licitações, de maneira que a fragmentação em itens acarretaria a perda do conjunto; perda da econômica de escala; redundaria em prejuízo à celeridade da licitação; ocasionaria a excessiva pulverização de contratos ou resultaria em contratos de pequena expressão econômica.

a) Do agrupamento por lote de itens que guardem homogeneidade entre si.

Nas licitações de objetos divisíveis o Tribunal de Contas da União entende que o julgamento seja feito por item, e não por preço global. Contudo, há situações em que se faz necessário aglutinar os itens com o intento de casar aquisições, visto que poderá haver um vínculo entre eles, ou se comprados separadamente prejudicarão o resultado esperado pela Administração.

Nesse caso, apesar dos objetos serem divisíveis, eles guardam estrita identidade de natureza e características semelhantes, além de guardar correspondência com sua composição, podendo cada lote ser fornecido por um mesmo fornecedor, por se tratarem de objetos comuns ao ramo de empresa de comercialização de Serviços de Telecomunicação e Serviços de Transmissão de dados, concretizando, assim, os princípios da competitividade.

b) Da fragmentação em itens acarretar a perda do conjunto.

O parcelamento do objeto somente se justifica e fundamenta quando houver viabilidade técnica e, principalmente, ganho econômico para a Administração Pública. No presente caso não há viabilidade técnica, uma vez que a falta de um componente prejudicaria todo o conjunto, de nada adiantaria ter a Internet Dedicada, sem ter o sistema de transmissão, como por exemplo. Há necessidade que todos os itens estejam disponíveis para o funcionamento do Sistema.

c) Da perda da economia de escala.

O § 1° do art. 23, da Lei n. 8.666/1993 determina que as compras efetuadas pela Administração sejam divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

Quanto maior a quantidade a ser comprada, maior poderá ser o desconto na compra de bens e serviços. Esse ganho está relacionado com o aumento da quantidade adquirida sem um aumento proporcional no custo e está intrinsicamente relacionado ao princípio da economicidade esculpido no art. 70 de nossa Carta Magna.

A economia de escala é definida como aquela que ocorre a partir de determinado patamar de quantidade de itens comercializados e pode acarretar relevante desconto na aquisição dos bens e serviços.

De tal modo, que no caso em tela a adoção critério de julgamento menor preço por lote permite o melhor aproveitamento dos recursos disponíveis no mercado e a ampliação da competitividade, sem perda da economia de escala, como por exemplo, a empresa que ganhar o lote fornecerá todos os itens, acarretando, consequentemente, uma diminuição nos custos e economia de escala.

d) Do prejuízo à celeridade da licitação.

Um dos fatores que pode ser levado em conta na elaboração de um edital por lote é o interesse na celeridade do processo.

Neste caso, trata-se de 3 lotes, assim, a contratação dos serviços por lotes, nos dará no máximo 03 empresas, o que não prejudicará a celeridade no julgamento das propostas. Caso contrário, se transformamos em itens, teríamos que estabelecer vários prazos entre várias empresas para conclusão do objeto contratado, e com isso, poderia haver um grande embaraço.

e) Da pulverização de contratos.

A licitação por itens corresponde, na verdade, a uma multiplicidade de licitações, cada qual com existência própria e dotada de autonomia jurídica, mas todas desenvolvidas conjugadamente em um único procedimento, documentado nos mesmos autos. Esta exagerada divisão de objeto pode ocasionar uma excessiva pulverização dos contratos, tornando mais dispendiosa a contratação.

Por outro lado, neste caso a adoção do critério de julgamento menor preço por lote para a Contratação de empresa de Telecomunicações especializadas para prestação de Serviços Continuado de: Comunicação dedicada para acesso à rede mundial de computadores- Internet- na modalidade terrestre suportando aplicações TCP/IP, resultaria na contratação de no máximo 03 empresas fornecedora/licitante, não ocorrendo a pulverização de contratos. Ainda há, com base no interesse público, maior segurança ao cumprimento do contrato.

Por fim, há que se observar o caso concreto, avaliando a conveniência e oportunidade, de modo a satisfazer da melhor forma o interesse público, pois cada contratação tem suas especificidades, *in casu* a aquisição por lote é mais vantajosa para a Administração, em decorrência dos riscos inerentes à própria execução, pois, não restam dúvidas, o objeto pretendido, quando executado por inúmeros contratados, poderá não ser integralmente entregue, tendo em vista problemas na relações jurídicas mantidas com diversos contratados.

f) Dos contratos de pequena expressão econômica.

Em razão da adoção do critério de menor preço por lote, não será celebrado contrato de pequena expressão econômica. Em caso contrário a licitação por itens sim geraria a situação de celebrar vários contratos de pequena expressão econômica.

3.2. OBJETIVO A SER ALCANÇADO:

3.2.1. Para dar continuidade na utilização dos Sistemas Automatizados do Poder Judiciário assim como a implantação de novas Comarcas, se faz necessária a interligação destas Comarcas com a Diretoria de Tecnologia da Informação, através de Links de dados usando padrão de tecnologia MPLS ou VPN IP SD-WAN podendo o acesso utilizar protocolos: SDH, Metro Ethernet ou GPON.

3.2.2. Através desta contratação, as interligações dos Prédios e de algumas Comarcas do Interior do Estado, poderão ter acesso aos Sistemas Computacionais alocados na sede do Poder Judiciário do Estado do Acre.

3.2.3. Garantir a aplicação dos princípios da segurança da informação, através de ferramentas com eficácias comprovadas no mercado de Tecnologia, suprindo assim as demandas de TIC do Poder Judiciário, bem como ampliando as soluções de segurança uma vez que atualmente existem legislações especificas quanto a proteção de dados pessoais.

3.2.4. Ampliar o acesso aos dispositivos móveis através de Redes Wifi com gestão centralizada, provendo conectividade e ao mesmo tempo gerenciamento dos recursos. Massificando ainda mais a utilização dos meios digitais de trabalho, otimizando as atividades e gerando economicidade com a transformação digital.

3.3. BENEFÍCIOS RESULTANTES:

3.3.1. Com a finalidade de oferecer ao Poder Judiciário do Estado do Acre, condições técnicas satisfatórias para prestação de serviços de telecomunicações bidirecionais, com possibilidade de aplicações de dados de forma dinâmica em âmbito corporativo, através de conexões dedicadas e Sistemas Comunicação de Dados, com abrangência nacional e possibilitando a conexão com outras redes públicas de dados do Brasil, pela CONTRATADA, no endereço da CONTRATANTE.

3.4. ALINHAMENTO ESTRATÉGICO:

3.4.1. O incremento nos custos de comunicação deve-se ao aumento da largura da banda de comunicação, tanto nas comunicações entre os Fóruns como o acesso à Internet.

3.4.2. A nova ampliação visa atender a resolução 211/2015 do CNJ Art. 24 Item VI, onde exige 2 (dois) Links de comunicação do órgão com a internet, mas com operadoras distintas para o acesso à rede de dados, com o máximo de comprometimento de banda de 80%, como é demonstrado nos GRUPO 1 e GRUPO 2, do Termo de Referência. Visa ainda atender a Resolução CNJ 370/2021 que não anula as ações/iniciativas do TJAC para atender os requisitos mínimos do nivelamento tecnológico da infraestrutura de TIC, conforme recomendado na Resolução 211/2015 no Art. 24 item VI, conforme deliberado na reunião com CNJ, em 10/03/2021, constante no SEI 0000550-59.2021.0000 item 18 (0944980):

"*Com A Revogação da Res. CNJ nº 211/2015 e a publicação da Res. CNJ nº 370/2021 novas estratégias foram traçadas. Entendemos que pelo bem da Administração Pública, as estratégias passadas se tornaram boas práticas que merecem ser continuadas ou mesmo aperfeiçoadas.*"

3.4.3. O objetivo deste Termo de Referência encontra respaldo no Planejamento Estratégico de TI (PDTIC), estando inserido especificamente no Plano de Continuidade de Serviços de TI.

3.4.4. O presente projeto faz parte do conjunto de ações de TI que serão desenvolvidas pela Diretoria de Tecnologia da Informação e está previsto no Plano de Aquisições e Contratações de TI.

3.5. ESCOLHA DA MODALIDADE:

3.5.1. Escolha da Modalidade: Tendo em vista as necessidades apresentadas e com fulcro na obtenção da proposta mais vantajosa para este Tribunal, sugere-se utilizar o PREGÃO ELETRÔNICO, pelo modo de disputa ABERTO como modalidade preferencial, conforme preceitua a Lei nº 10.520, de 17 de julho de 2002, Decretos Federais nº 3.555/2000, 10.024/2019 e o Decreto Estadual nº 4.767/2019, aplicando-se subsidiariamente, as disposições da Lei nº 8.666/1993.

3.6. Considerando tratar-se de serviço de duração continuada, a contratação decorrente deste Termo de Referência deverá ter validade de 12 (doze) meses, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

3.6.1. Os serviços tenham sido prestados regularmente;

3.6.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

3.6.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

3.6.4. Haja manifestação expressa da contratada informando o interesse na prorrogação;

3.6.5. Seja comprovado que o contratado mantém as condições iniciais de habilitação.

4. INSTALAÇÃO, IMPLEMENTAÇÃO, SUPORTE TÉCNICO E MUDANÇA DE LINKS:

4.1. LOCAL E EXECUÇÃO DOS SERVIÇOS

4.1.1. A instalação da solução deverá ser executada na sede da CONTRATANTE;

4.1.2. Os serviços de monitoração e gerenciamento da solução deverão ser prestados de forma remota pela CONTRATADA, em suas instalações;

4.1.3. Os serviços de instalação deverão ser realizados, durante o horário comercial, de segunda à sexta-feira, das 8h30 às 17h30 do horário local da execução da instalação, e exceto nos casos que afetem os sistemas em produção, caso em que deverão ser agendados com antecedência.

4.2. Da instalação e implementação:

4.2.1. A Solução deve ser fornecida com os componentes necessários para sua completa instalação e o perfeito funcionamento da solução.

4.2.2. A CONTRATADA deverá disponibilizar os serviços para os links, no prazo de até 60 (sessenta) dias corridos, contados do recebimento da ordem de serviço.

- Em caso de necessidade de elaboração de projeto específico para viabilizar a infraestrutura necessária à prestação do serviço, o prazo de entrega do serviço poderá ser prorrogado por igual período mediante justificativa da contratada, a ser entregue antes de findar o prazo inicial.

4.3. Do suporte técnico:

4.3.1. O suporte técnico deverá ser prestado 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o período de vigência do contrato e o atendimento deverá ocorrer imediatamente após a abertura do chamado técnico, no qual deverá ser fornecido um número de registro de chamado técnico.

4.4. Da mudança de links:

4.4.1. Durante o período de vigência do contrato, caso haja mudança física e/ou de velocidade nas instalações do Tribunal de Justiça do Estado do Acre, a Contratada deverá reinstalar e ativar os links.

4.4.2. As mudanças físicas e/ou de velocidade dos links cotados deverão ser solicitadas por escrito pela Contratante, num prazo mínimo de 10 (dez) dias de antecedência.

4.4.3. A Contratada deverá se manifestar num prazo máximo de 10 (dez) dias, após recebimento do comunicado, através de relatório técnico da viabilidade ou não da mudança física e/ou de velocidade dos links. Caso a Contratada não se manifeste no prazo estipulado, serão consideradas como aceitas as mudanças solicitadas.

4.4.4. Caso a Contratada comprove no relatório técnico que não é possível fazer a mudança física dos links nas mesmas condições definidas neste Edital, a mesma deverá apresentar proposta para nova instalação.

4.4.5. A Contratada deverá comunicar por escrito, devidamente justificado, o aceite ou não da nova instalação física e/ou de velocidade dos links, bem como sua supressão ou não da fatura mensal.

4.4.6. Tendo sido aceito a nova instalação, a CONTRATADA deverá mudar os links, no prazo de até 30 (trinta) dias corridos, contados do recebimento da ordem de serviço.

4.4.7. Os roteadores instalados e configurados neste Tribunal poderão ser substituídos por equipamentos fornecidos pelo mesmo, sendo o custo dos mesmos subtraídos da fatura mensal.

4.4.8. Quando da substituição dos equipamentos da Contratada, pelos fornecidos pelo Tribunal, a instalação e configuração dos mesmos deverão ser feitas obrigatoriamente em conjunto entre ambos, com emissão de relatórios assinado por ambas as partes de todas as configurações feitas.

4.5. Do treinamento para soluções de segurança e gerenciamento:

4.5.1. Deverá ser fornecido treinamento na solução integrada de segurança, WIFI e WAF adquirida, de no mínimo 20 (vinte) horas, para até 4 (quatro) pessoas, designadas pela CONTRATANTE, em até 15 (quinze) dias após término da instalação, a fim de repassar as informações necessárias dos produtos adquiridos, incluindo detalhamento dos produtos e seus aspectos gerais de configuração e operação;

4.6. Do licenciamento de software dos equipamentos

4.6.1. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos, seja ele utilizado de forma virtual ou física, local ou em nuvem;

5. CARACTERÍSTICAS DOS SERVIÇOS DE INTERNET PARA GRUPO 1 ITEM 01 E GRUPO 2 ITEM 01

5.1. O serviço dedicado de acesso à internet tem como característica prover o serviço de acesso à Internet com segurança integrada para a infraestrutura de rede da CONTRATANTE;

5.2. Os serviços deverão ser providos por meio de acesso terrestre (metálicos ou cabos óticos) a redes estatísticas ou determinísticas, compatíveis com as especificações exigidas neste Termo de Referência;

5.3. Os links de acesso à Internet não poderão ser compartilhados com nenhum outro cliente do prestador de serviços e deverão possuir dimensionamento correto para garantir a transmissão de dados de acordo com a velocidade estipulada neste instrumento, bem como garantir a qualidade de serviços mínima exigida;

5.4. Todos os equipamentos e acessórios necessários para a ativação dos links de acesso à Internet deverão ser fornecidos pela CONTRATADA e seguirão as características técnicas dispostas neste documento;

5.5. Os serviços deverão permitir modificações ou ampliações sem que estas impliquem na interrupção do restante das conexões da rede;

5.6. Mudanças de endereço deverão ser realizadas sempre que solicitado mediante viabilidade técnica, sem ônus para a CONTRATANTE;

5.7. Quaisquer alterações relativas aos serviços de acesso de dados serão informadas pela CONTRATANTE, por meio de documento próprio, a ser definido após a assinatura do contrato;

5.8. Todos os links de acessos deverão ser entregues em pleno funcionamento conforme abaixo:

5.8.1. Deverão ser fornecidos todos os equipamentos necessários à prestação do serviço tais como modens, roteadores e outros necessário sem ônus para a CONTRATANTE;

5.8.2. Serviços de implantação dos pontos de acesso à Internet, incluindo todo o preparo para a entrega dos links;

5.8.3. Serviços de instalação em todas as localidades indicadas neste instrumento dos equipamentos fornecidos pela CONTRATADA;

5.8.4. Serviços de gerência proativa da rede;

5.8.5. Serviços de configuração dos equipamentos fornecidos;

5.8.6. Serviços de integração e testes de cada link fornecido;

5.8.7. Serviços de manutenção dos links, com substituição em caso de defeito nos equipamentos, garantindo a continuidade do serviço, sem custo adicional;

5.8.8. Serviços esporádicos relativos ao remanejamento de links, juntamente com seus equipamentos.

5.9. Os serviços fornecidos deverão ter as características técnicas conforme especificações constantes neste instrumento;

5.10. Todos os serviços de link dedicado, incluindo o atendimento técnico, devem estar disponíveis no período de 24 horas por dia, 7 (sete) dias por semana, por todo o período contratado, exceto nas interrupções programadas em razão de situações de emergência, motivadas por razões de ordem técnica ou por razões de segurança das instalações.

5.11. Caso haja necessidade de interrupção dos serviços, inclusive em função de mudança de tecnologia, a CONTRATADA deverá comunicar, por escrito, com antecedência mínima de 7 (sete) dias úteis, podendo ser deferido ou não o pedido, dependendo da conveniência e interesse da CONTRATANTE;

5.12. Essas interrupções só poderão ocorrer nos finais de semana, entretanto, caso a CONTRATADA exceda o período previsto, o referido serviço será considerado indisponível no tempo excedente;

5.13. Os serviços serão considerados disponíveis desde que estejam plenamente funcionais e operacionais, atendendo a todas as especificações técnicas referentes ao respectivo serviço. Entretanto, o serviço não será considerado indisponível em razão de fatos que estejam sob a responsabilidade da CONTRATANTE;

5.14. Os níveis de acordo de serviço mínimos – SLA – especificados neste projeto consideram a continuidade das atividades que dependem especificamente do acesso à internet para a qualidade no atendimento prestado aos assistidos da CONTRATANTE;

5.15. O Backbone do prestador de serviço de link dedicado deve:

5.15.1. Possuir canais próprios e dedicados;

5.15.2. Dispor de um bloco contínuo de, no mínimo, 254 (duzentos e cinquenta e quatro) números IPs próprios/públicos e válidos na Internet para o ITEM 01 do GRUPO 1 e de, no mínimo, 254 (duzentos e cinquenta e quatro) números IPs próprios/públicos e válidos na Internet para o ITEM 01 do GRUPO 2.

5.15.3. Fornecer o serviço de DNS Secundário e Reverso nas suas instalações;

5.15.4. O serviço DNS deverá suportar o protocolo DNSSEC;

5.15.5. Deve possuir política de roteamento que permita trânsito nacional e internacional para a CONTRATANTE;

5.15.6. Fornecer toda a infraestrutura (ECDs, enlaces de comunicação, etc.) necessária para atender os requisitos especificados neste Termo de Referência, incluindo a configuração, manutenção e gerenciamento;

5.15.7. Fornecer o roteador para a prestação dos serviços com todos os acessórios e programas necessários à sua instalação, operação e monitoração, sendo que o roteador deverá possuir no mínimo Possuir, no mínimo, 01 (uma) porta óptica de acordo com os Standarts ITU-G.984 GPON; possuir, no mínimo, 04 (quatro) Gigabit Ethernet 10/100/1000 de detecção automática que sejam compatíveis com os padrões ISSO 8802.3 e IEE 802.3; a interface física da porta LAN deverá ser fornecida no padrão RJ-45 (10baseT), para cabos UTP, CAT 6 ou AUI; possuir opção de boot local via memória flash ou similar; permitir ser alimentado de forma automática por tensões de 110/220 VAC, frequência 60 Hz com duas fontes redundantes; deverá suportar e implementar serviços de DHCP Server; deverá ser gerenciável via SNMP;

5.16. Como garantia de disponibilidade de acesso aos sistemas institucionais da CONTRATANTE e à Internet a CONTRATADA deverá, necessariamente, possuir e comprovar, no mínimo, 2 (dois) POP's (Ponto de Presença) próprios no estado do Acre que utilizem tecnologia ATM, SDH ou Gigabit Ethernet para conexão com a rede mundial de computadores, sendo entes POPs. Inclui-se obrigatoriamente um POP na cidade de Rio Branco - AC, onde encontra-se a sede administrativa da CONTRATANTE e seu site tecnológico (estrutura de serviços e servidores).

5.17. Será permitido a CONTRATADA o uso de "trunking", ou seja, o uso de mais de um enlace para compor a velocidade contratada, desde que seja realizado por equipamento próprio sem ônus para a CONTRATANTE e devidamente configurado, entregando o link na sua velocidade contratada de forma transparente;

5.18. A LICITANTE deverá possuir no mínimo o dobro do valor da banda do link dedicado entre o POP da contratada com o backbone nacional de Internet (AS/NAP);

5.19. O backbone da CONTRATADA deverá possuir pelo menos 01 (uma) saída internacional própria, ou contratados para seu uso.

5.20. O backbone da CONTRATADA deverá possuir interligação direta através de canais próprios e dedicados, a pelo menos 3 (três) outros AS (além das conexões descritas no item anterior), com peering BGP IPv4 e IPv6. As bandas de saída entre referidos AS deverão somar pelo menos 10 Gbps (dez gigabits por segundo).

5.21. A licitante do serviço deverá possuir Termo de Autorização da Agência Nacional de Telecomunicações – ANATEL, bem como o registro de suas estações.

6. SERVIÇO DE PROTEÇÃO NO BACKBONE CONTRA ATAQUES DDOS PARA O GRUPO 1 ITEM 01 E GRUPO 2 ITEM 01

6.1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (Denial of Service) e DDOS (Distributed Denial of Service);

6.2. A CONTRATADA deve disponibilizar pelo menos um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

6.3. O acesso à Internet (circuito de dados) não poderá ser subcontratado de terceiros, devendo a CONTRATADA fornecer ambos os serviços, solução ANTI-DDOS e circuito de dados.

6.4. A técnica ANTI-DDOS utilizada deverá ser por métrica de volumetria, assim a contratada deverá enviar junto com a proposta técnica, qual a estratégia utilizada para mitigação de ataques DDOS sobre o circuito de dados.

6.5. A solução ANTI-DDOS deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (DDoS – Distributed Denial of Service) ou não;

6.6. A CONTRATADA deve possuir e disponibilizar no mínimo 2 (dois) centros de limpeza nacional cada um com capacidade de mitigação de no mínimo 40Gbps e no mínimo 1 (um) por centro de limpeza internacional com capacidade de mitigação de no mínimo 80Gbps.

6.7. Não haverá taxa adicional por volume de mitigação de ataques (DDoS – Distributed Denial of Service) nos IP's monitorados;

6.8. A alteração de capacidade de mitigação deverá ser implementada em um prazo máximo de 5 dias úteis, a contar da data de solicitação formal através de correio eletrônico encaminhado via chave oficial ou de autorizados pelo TRIBUNAL DE JUSTIÇA DO ACRE.

6.9. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo CONTRATANTE continuem disponíveis;

6.10. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;

6.11. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

6.12. A CONTRATADA deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo;

6.13. Para a mitigação dos ataques o tráfego só deverá ser encaminhado para limpeza fora do território brasileiro nos casos em que os centros nacionais não suportarem a capacidade de mitigação e a demanda de ataques, no restante os ataques de origem nacional deverão ser tratados nos centros nacionais e os de origem internacional nos centros internacionais;

6.14. O envio de tráfego para mitigação em centros internacionais deverá ser justificado em relatório.

6.15. Nos períodos de ataque a latência do circuito deverá ser de no máximo 150 ms (milissegundos) quando a mitigação se originar dos centros de limpeza nacionais e de no máximo 250 ms (milissegundos) quando se originar do(s) centro(s) internacionais.

6.16. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

6.17. A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da contratante para coleta dos dados a serem analisados;

6.18. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

6.19. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro por um determinado cliente;

6.20. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP/HTTPS, DNS, VPN, FTP, NTP, UDP, ICMP, correio eletrônico, bloqueio por localização geográfica de endereços IP, dentre outras;

6.21. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4, incluindo, mas não se restringindo aos seguintes:

- Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
- Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
- Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
- Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

6.22. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada;

6.23. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

6.24. Realizar a comunicação da ocorrência do ataque à CONTRATANTE imediatamente após a detecção;

- A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;
- Outras configurações deverão ser possíveis, como exemplo monitoração de um cliente por sub-interface no PE;

6.25. A CONTRATADA deverá disponibilizar relatórios mensais de mitigação de ataques, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação, horário de sucesso da mitigação e horário de fim do ataque. Em conjunto com o relatório mensal relatórios dinâmicos deverão ser disponibilizados em até 48 horas após um ataque por solicitação da CONTRATANTE.

6.26. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada;

6.27. A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra ataques DDOS (Distributed Denial of Service).

6.28. A CONTRATADA deverá apresentar relatório analítico, enviado mensalmente ao cliente;

6.29. A CONTRATADA terá no máximo 15 minutos para iniciar a mitigação de ataques de DOS e DDOS;

6.30. A interface digital a ser conectada no backbone do TRIBUNAL DE JUSTIÇA DO ACRE deverá seguir o padrão Gigabit Ethernet.

6.31. Os serviços ofertados deverão operar no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

6.32. O backbone IP do provedor deve ter saída com destino direto a outros provedores de backbone IP Nacionais de nível Tier 1, 2 e 3, com banda de 100 Gbps no mínimo.

7. CARACTERÍSITICAS DOS SERVIÇOS – REDE TJAC.NET:

7.1. A rede TJAC será composta pelos Links listados nos GRUPO 1 e GRUPO 2, deste Termo de Referência.

7.2. A LICITANTE deverá fornecer senha de acesso com direito a acesso (leitura) dos equipamentos, a fim de proporcionar à TJAC ferramentas de avaliação técnica dos mesmos, proporcionando adoção de ações preventivas ou corretivas.

7.3. Os equipamentos (roteadores), fornecidos pela LICITANTE deverão estar com SNMP, COMUNIDADE, RMON e TRAP habilitados para leitura, de sorte a proporcionar ao TJAC ferramentas de avaliação técnica dos mesmos, proporcionando adoção de ações preventivas ou corretivas.

7.4. O Link Concentrador deverá ser entregue pela CONTRATADA em um único meio físico, sem fracionar (Mux, Modem Óptico ou outro equipamento).

7.5. Seguir o padrão DSCP (DiffServ Code Point), RFC 2474.

7.6. Possuir suporte à tradução de endereços IP (NAT).

7.7. Possuir suporte a classe de serviço para, fragmentação de pacotes.

7.8. Possuir suporte a classe de serviço para, reserva de banda.

7.9. Possuir suporte a classe de serviço para, listas de controle de acesso.

7.10. A topologia da rede TJAC deverá ser full-mesh.

7.11. Os serviços de Intranet são os acessos à Rede Virtual Privada (VPN), a ser criada pela CONTRATADA em seu backbone IP/MPLS, por onde fruirá o tráfego de dados entre as diversas unidades do CONTRATANTE.

7.12. Garantir o roteamento das conexões dedicadas utilizando protocolo MPLS – Multiprotocol Label Switching.

7.13. Cada acesso não poderá ser compartilhado com nenhum outro cliente da CONTRATADA e deverá ser capaz de absorver 100% (cem por cento) do tráfego referente à velocidade contratada;

7.14. O uso de “trunking”, ou seja, o uso de mais de um enlace para atingir a velocidade desejada do link contratado será permitido.

7.15. Operar em conformidade com, no mínimo, as seguintes RFCs:

7.15.1. RFC 3031: “Multiprotocol Label Switching Architecture”;

7.15.2. RFC 3032: “MPLS Label Stack Encoding”;

7.15.3. RFC 3270: “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services”;

7.15.4. RFC 2474: “Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers”;

7.15.5. RFC 2475: “An Architecture for Differentiated Services”;

7.16. Os equipamentos instalados em todos os acessos da rede deverão realizar a marcação de pacotes com vistas à priorização de dados provenientes dos seguintes aplicativos:

7.17. Permitir a classificação e marcação de diferentes níveis de tráfego (CoS e QoS), sendo implementadas as seguintes classes de serviço:

7.17.1. Tempo Real Voz e/ou Vídeo: Aplicações sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem a priorização de pacotes de dados e reserva de banda na rede;

7.17.2. Dados Prioritários: Aplicações interativas, que exigem entrega garantida e tratamento prioritário. São os dados envolvidos nas aplicações essenciais às atividades fins do CONTRATANTE;

7.17.3. Dados Comuns (mínimo 25% da banda total do acesso): Aplicações com mensagens de tamanho muito variado e não imprescindíveis às atividades fins do CONTRATANTE, aplicativos de dados que não necessitam de priorização, como páginas WEB, e-mails. Para esta classe a rede deverá permitir o fluxo do tráfego de dados por meio da técnica Best Effort e impedindo que esse tráfego afete negativamente as demais classes;

7.18. A banda a ser definida para cada classe de serviço em cada acesso da rede será acordada futuramente entre o CONTRATANTE e a CONTRATADA, quando da solicitação do serviço;

7.19. O serviço contratado deverá permitir modificações ou ampliações sem que estas impliquem na interrupção do restante das conexões da rede;

7.20. Poderão ser solicitados, durante a vigência do contrato, novos acessos, alterações de velocidade, de tipo, de classes de serviços ou mudanças de endereço;

7.21. Quaisquer alterações dos serviços serão solicitadas pelo CONTRATANTE, através de documento próprio a ser definido após a assinatura do contrato;

7.22. É de responsabilidade do CONTRATANTE definir o endereçamento IP da rede, bem como suas regras de roteamento;

7.23. Caso o CONTRATANTE necessite alterar o endereçamento IP e/ou as regras de roteamento, o prazo de atendimento será acordado entre as partes e a solicitação será mediante ofício entregue a CONTRATADA;

8. DETALHAMENTO SOLUÇÃO DE SEGURANÇA DE PERIMETRO NGFW

8.1. Equipamento CPE Segurança NGFW TIPO 1 (2 unidades CLUSTER) – Sede do Tribunal de Justiça (DITEC).

8.1.1. Throughput de, no mínimo, 5 Gbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;

8.1.2. Thoughput de, no mínimo, 4.7 Gbps para Controle de Aplicação;

8.1.3. Throughput de, no mínimo, 36 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

8.1.4. Suporte a, pelo menos, 8 milhões de sessões concorrentes TCP;

8.1.5. Suporte a, pelo menos, 300 mil novas sessões TCP por segundo;

8.1.6. Suportar no mínimo 5.7 Gbps de throughput de Inspeção SSL;

8.1.7. Throughput de, no mínimo, 7.9 Gbps de IPS;

8.1.8. Throughput de, no mínimo, 20 Gbps de VPN IPSec;

8.1.9. Throughput de, no mínimo, 5 Gbps de VPN SSL;

8.1.10. Suportar pelo menos 2.000 tuneis IPSec Site-to-Site

8.1.11. Suportar pelo menos 50.000 tuneis IPSec Site-to-Client

8.1.12. Possuir ao menos 8 interfaces SFP Gigabit Ethernet, 2 interfaces SFP+, 8 interfaces RJ45 Gigabit Ethernet, 2 interfaces RJ45 para gerenciamento e Alta Disponibilidade (HÁ);

8.1.13. Suportar a criação de no mínimo 10 instâncias virtuais;

8.1.14. Deve suportar a instalação em rack padrão 19”ou ser entregue com bandeja para a instalação em rack;

8.1.15. Fontes redundantes, hot swap;

8.1.16. Deve estar homologado na ANATEL até a data da licitação;

8.2. Equipamento CPE Segurança NGFW TIPO 2 – Links Interurbanos Comarcas do Tribunal de Justiça

8.2.1. Throughput de, no mínimo, 220 Mbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;

8.2.2. Thoughput de, no mínimo, 450 Mbps para Controle de Aplicação;

8.2.3. Throughput de, no mínimo, 2.5 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

8.2.4. Suporte a, pelo menos, 1.8 Milhões de sessões concorrentes TCP;

8.2.5. Suporte a, pelo menos, 21 mil novas sessões TCP por segundo;

8.2.6. Suportar no mínimo 150 Mbps de throughput de Inspeção SSL;

8.2.7. Throughput de, no mínimo, 350 Mbps de IPS;

8.2.8. Throughput de, no mínimo, 90 Mbps de VPN IPSec;

8.2.9. Throughput de, no mínimo, 100 Mbps de VPN SSL;

8.2.10. Possuir ao menos 5 interfaces RJ45 Gigabit Ethernet;

8.2.11. Possuir ao menos 1 interfaces RJ45 para gerenciamento

8.2.12. Deve estar homologado na ANATEL até a data da licitação;

8.3. Equipamento CPE Segurança NGFW TIPO 3 – Links Interurbanos Comarcas do Tribunal de Justiça

8.3.1. Throughput de, no mínimo, 200 Mbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;

8.3.2. Thoughput de, no mínimo, 400 Mbps para Controle de Aplicação;

8.3.3. Throughput de, no mínimo, 950 Mbps para Firewall, considerando pacotes UDP de 1518 bytes;

8.3.4. Suporte a, pelo menos, 900 mil sessões concorrentes TCP;

8.3.5. Suporte a, pelo menos, 15 mil novas sessões TCP por segundo;

8.3.6. Suportar no mínimo 125 Mbps de throughput de Inspeção SSL;

8.3.7. Throughput de, no mínimo, 300 Mbps de IPS;

8.3.8. Throughput de, no mínimo, 75 Mbps de VPN IPSec;

8.3.9. Throughput de, no mínimo, 35 Mbps de VPN SSL;

8.3.10. Possuir ao menos 5 interfaces RJ45 Gigabit Ethernet;

8.3.11. Possuir ao menos 1 interfaces RJ45 para gerenciamento

8.3.12. Deve estar homologado na ANATEL até a data da licitação;

8.4. Características gerais para todos os equipamentos NGFW

8.4.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

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

8.4.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

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

8.4.5. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

8.4.6. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.4.7. Deve suportar BGP, OSPF, RIP e roteamento estático;

8.4.8. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

8.4.9. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

8.4.10. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

8.4.11. Deve suportar NAT dinâmico (Many-to-Many);

8.4.12. Deve suportar NAT estático (1-to-1);

8.4.13. Deve suportar NAT estático bidirecional 1-to-1;

8.4.14. Deve suportar Tradução de porta (PAT);

8.4.15. Deve suportar NAT de Origem;

8.4.16. Deve suportar NAT de Destino;

8.4.17. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

8.4.18. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

8.4.19. Deve suportar NAT64;

8.4.20. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

8.4.21. Enviar log para sistemas de monitoração externos;

8.4.22. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

8.4.23. Proteção anti-spoofing;

8.4.24. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

8.4.25. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.4.26. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

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

8.4.28. Controle, inspeção e decriptografia de SSL para tráfego de Saída (Outbound);

8.4.29. A solução deve suportar integração nativa com Let’s Encrypt, para obtenção de certificados válidos, de forma automática;

8.4.30. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

8.4.31. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

8.5. Políticas

8.5.1. Deverá suportar controles por zonas de segurança;

8.5.2. Deverá suportar controles de políticas por porta e protocolo;

8.5.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

8.5.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.5.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

8.5.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

8.5.7. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

8.5.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

8.5.9. Suporte a objetos e regras IPV6;

8.5.10. Suporte a objetos e regras multicast;

8.5.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

8.6. Controle de Aplicações

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

8.6.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

8.6.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

8.6.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

8.6.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

8.6.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

8.6.7. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

8.6.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

8.6.9. Identificar o uso de táticas evasivas via comunicações criptografadas;

8.6.10. Atualizar a base de assinaturas de aplicações automaticamente;

8.6.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

8.6.12. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

8.6.13. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

8.6.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

8.6.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

8.6.16. Deve alertar o usuário quando uma aplicação for bloqueada;

8.6.17. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

8.6.18. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

8.6.19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

8.6.20. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

8.6.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

8.6.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;

8.6.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

8.6.24. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

8.6.25. Deve permitir o filtro de vídeos que podem ser visualizados no YouTube;

8.7. Prevenção de ameaças

8.7.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

8.7.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

8.7.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

8.7.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

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

8.7.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

8.7.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

8.7.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

8.7.9. Deve permitir o bloqueio de vulnerabilidades;

8.7.10. Deve permitir o bloqueio de exploits conhecidos;

8.7.11. Deve incluir proteção contra-ataques de negação de serviços;

8.7.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

8.7.13. Detectar e bloquear a origem de portscans;

8.7.14. Bloquear ataques efetuados por worms conhecidos;

8.7.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

8.7.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

8.7.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

8.7.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

8.7.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

8.7.20. Identificar e bloquear comunicação com botnets;

8.7.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

8.7.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

8.7.23. Os eventos devem identificar o país de onde partiu a ameaça;

8.7.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

8.7.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

8.7.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas

políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

8.7.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

8.7.28. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

8.7.29. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

8.7.30. Para o firewall concentrador, aplica-se apenas os recursos de IPS descritos nesse grupo de itens. Para o firewall das pontas remotas, aplica-se todos os requisitos descritos nesse grupo de itens;

8.8 Filtro de URLs

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

8.8.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

8.8.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.8.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

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

8.8.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

8.8.7. Possuir pelo menos 60 categorias de URLs;

8.8.8. Deve possuir a função de exclusão de URLs do bloqueio;

8.8.9. Permitir a customização de página de bloqueio;

8.8.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

8.8.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

8.8.12. Os requisitos de filtro de URL descritos acima aplicam-se apenas ao firewall;

8.9. Identificação de usuários

8.9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

8.9.2. 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;

8.9.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

8.9.4. 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, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

8.9.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

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

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

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

8.9.9. Deve suportar o envio e recebimento de credenciais via RADIUS;

8.10. Filtro de dados

8.10.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

8.10.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

8.10.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

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

8.11. Geolocalização

8.11.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

8.11.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

9. RECURSOS GERAIS DE SD-WAN

9.1.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

9.1.2. Deve ser possível criar políticas que definam os seguintes critérios para match:

9.1.2.1. Endereços de origem;

9.1.2.2. Grupos de usuários;

9.1.3. Endereços de destino;

9.1.4. DSCP;

9.1.5. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

9.1.6. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

9.1.7. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente, inclusive 4G;

9.1.8. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

9.1.9. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

9.1.10. A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

9.1.11. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

9.1.12. A solução deve permitir a definição do roteamento para cada aplicação;

9.1.13. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

9.1.14. Deve possibilitar a definição do link de saída para uma aplicação específica;

9.1.15. Deve implementar balanceamento de link por hash do IP de origem;

9.1.16. Deve implementar balanceamento de link por hash do IP de origem e destino;

9.1.17. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

9.1.18. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

9.1.19. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

9.1.20. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

9.1.21. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

9.1.22. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

9.1.23. A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;

9.1.24. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

9.1.25. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

9.1.26. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

9.1.27. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;

9.1.28. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

9.1.29. O QoS deve possibilitar a definição de fila de prioridade;

9.1.30. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

9.1.31. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

9.1.32. Deve possibilitar a definição de bandas distintas para download e upload;

9.1.33. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

9.1.34. A solução de SD-WAN deve suportar IPv6;

9.1.35. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

9.1.36. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

9.1.37. O SD-WAN deverá possuir serviço de Firewall Stateful;

9.1.38. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

9.1.39. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

9.1.40. Deve ser capaz de bloquear acesso às aplicações;

9.1.41. Deve suportar NAT dinâmico bem como NAT de saída;

9.1.42. Deve suportar balanceamento de tráfego por sessão e pacote;

9.1.43. Suportar VPN IPSec Site-to-Site;

9.1.44. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

9.1.45. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

9.1.46. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

9.1.47. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

9.1.48. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

9.1.49. Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPs dinâmicos;

9.1.50. Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;

9.1.51. Deve possuir suporte e estar licenciamento para uso de VRFs;

10.0. GERENCIAMENTO CENTRALIZADO

10.0. Gerenciamento Centralizado

10.0.1. Considerando o volume de equipamentos e escala do projeto, faz-se necessária uma solução de gerenciamento dos equipamentos ofertados;

10.0.2. O fornecedor deve considerar recursos de gestão centralizada para as soluções NGFW, SD-WAN;

10.0.3. Devem ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados;

10.0.4. Deve considerar o volume de equipamentos ofertados, considerando todo o licenciamento necessário para a correta gestão dos elementos de rede;

10.0.5. Pode ser ofertado em VM, desde que compatível com VMware ESXI 5.5 e acima, Hyper-V 2008 e acima e KVM;

10.0.6. Pode ser ofertado em hardware, desde que em appliance do próprio fabricante;

10.0.7. A solução de gerencia centralizada deve ser capaz de gerenciar pelo menos 100 dispositivos de segurança e possibilitar pelo menos o armazenamento de 5 GB de LOG diariamente.

10.0.8. A gerencia centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento de gerenciamento centralizado, ou fornecido em equipamento externo do mesmo fabricante;

10.0.9. A solução de visualização de logs deve ser capaz de armazenar pelo menos 25GB de LOG diariamente, sendo possível visualizar log de pelo menos 10.000 dispositivos.

10.1. Gerencia Centralizada de NGFW

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

10.1.2. O sistema deverá suportar contas de usuário/senha estáticas;

10.1.3. Permitir acesso concorrente de administradores;

10.1.4. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

10.1.5. O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius;

10.1.6. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;

10.1.7. Essas comunicações deverão ser protegidas e criptografadas;

10.1.8. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;

10.1.9. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;

10.1.10. A console de Gerência deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN;

10.1.11. Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência;

10.1.12. Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN;

10.1.13. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

10.1.14. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

10.1.15. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

10.1.16. Permitir localizar quais regras um objeto está sendo utilizado;

10.1.17. Permitir criação de regras que fiquem ativas em horário definido;

10.1.18. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;

10.1.19. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

10.1.20. Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador;

10.1.21. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;

10.1.22. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;

10.1.23. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

10.1.24. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

10.1.25. Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

10.1.26. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;

10.1.27. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;

10.1.28. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

10.1.29. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

10.1.30. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

10.1.31. Permitir criar regras anti DDoS de forma centralizada;

10.1.32. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

10.1.33. Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;

10.1.34. Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;

10.1.35. Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes, etc.;

10.1.36. Deve oferecer portal personalizado para gerenciamento de dispositivos, APs, políticas e objetos, junto com painéis, relatórios e visualizações personalizadas para atualizações de segurança abrangentes, análises em tempo real e respostas exclusivas às suas necessidades;

10.1.37. O portal deve permitir uma visão geral do tráfego de rede e da postura de segurança, incluindo widgets intuitivos com informações como principais países, principais ameaças, principais origens de tráfego, principais destinos, principais aplicativos e hits de políticas, bem como gráficos para mostrar logins de administrador, eventos do sistema, e uso de recursos;

10.1.38. O portal deve suportar a sua configuração possibilite seu uso via multi-tenant, ou seja, com a possibilidade de se criarem vários portais de acesso independentes entre si para fins de administração distribuída;

10.1.39. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

10.1.40. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

10.1.41. A gerencia centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento de gerenciamento centralizado, ou fornecido em equipamento externo do mesmo fabricante;

10.1.42. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

10.1.43. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

10.1.44. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

10.1.45. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

10.1.46. Deve possuir mecanismos de remoção automática para logs antigos;

10.1.47. Permitir importação e exportação de relatórios;

10.1.48. Deve ter a capacidade de criar relatórios no formato HTML e CSV;

10.1.49. Deve permitir exportar os logs no formato CSV;

10.1.50. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

10.1.51. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

10.1.52. A solução deve ter relatórios predefinidos;

10.1.53. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

10.1.54. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

10.1.55. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

10.1.56. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

10.1.57. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

10.1.58. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

10.1.59. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

10.1.60. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

10.1.61. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

10.1.62. Permitir o envio por e-mail relatórios automaticamente;

10.1.63. Deve permitir que o relatório seja enviado por email para o destinatário específico;

10.1.64. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

10.1.65. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

10.1.66. Deve permitir o uso de filtros nos relatórios;

10.1.67. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

10.1.68. Permitir especificar o idioma dos relatórios criados;

10.1.69. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

10.1.70. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

10.1.71. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

10.1.72. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

10.1.73. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

10.1.74. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

10.1.75. Deve permitir visualizar em tempo real os logs recebidos;

10.1.76. Deve permitir o encaminhamento de log no formato syslog;

10.1.77. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

10.1.78. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

10.1.79. Deve permitir gerar alertas de eventos a partir de logs recebidos;

11.0. SOLUÇÃO DE GERENCIAMENTO E DISTRIBUIÇÃO SEM FIO

11.1. Gerenciamento centralizado

11.1.1. Serão aceitas soluções com controladoras locais, centralizada ou cloud, desde que atendam aos requisitos deste termo de referência;

11.1.2. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

11.1.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

11.1.4. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;

11.1.5. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

11.1.6. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e DNS;

11.1.7. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

11.1.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

11.1.9. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

11.1.10. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

11.1.11. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

11.1.12. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

11.1.13. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

11.1.14. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

11.1.15. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

11.1.16. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

11.1.17. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

11.1.18. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

11.1.19. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

11.1.20. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos
dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

11.1.21. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

11.1.22. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

11.1.23. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless;

11.1.24. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:

11.1.25. - Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);

11.1.26. - Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;

11.1.27. - ASLEAP;

11.1.28. - Null Probe Response or Null SSID Probe Response;

11.1.29. - Long Duration;

11.1.30. - Ataques contra Wireless Bridges;

11.1.31. - Weak WEP;

11.1.32. - Invalid MAC OUI.

11.1.33. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;

11.1.34. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;

11.1.35. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;

11.1.36. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

11.1.37. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

11.1.38. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

11.1.39. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

11.1.40. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

11.1.41. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

11.1.42. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

11.1.43. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as
credenciais válidas para acesso à rede;

11.1.44. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

11.1.45. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

11.1.46. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

11.1.47. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

11.1.48. A solução deve permitir a configuração do captive portal com endereço IPv6;

11.1.49. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

11.1.50. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

11.1.51. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

11.1.52. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

11.1.53. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

11.1.54. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

11.1.55. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

11.1.56. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

11.1.57. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos
seguintes formatos: JPEG, PNG, GIF ou CAD;

11.1.58. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

11.1.59. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

11.1.60. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

11.1.61. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

11.1.62. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

11.1.63. A solução ofertada deve possuir recursos para onboard seguro de dispositivos wireless, baseando-se em atributos dos elementos, tais como: usuários, mac-address, tipo, família, SO, hardware e fabricante, dentro outros;

11.1.64. Uma vez que seja um dispositivo reconhecido, ele deve ser colocado na respectiva vlan. Do contrário, permanecerá um vlan isolada;

11.1.65. A CONTRATADA disponibilizará central de atendimento especializado e personalizado para comunicação de falhas e inoperâncias do circuito/porta de acesso. O atendimento será prestado através de ligação telefônica gratuita via 0800, disponível 24 horas por dia, sete dias por semana;

11.2. Ponto de Acesso Wireless Wifi Tipo 1 - Indoor

11.2.1. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

11.2.2. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

11.2.3. O ponto de acesso deve possuir rádio Wi-Fi dedicado para executar funções de sensor com objetivo de identificar interferências e ameaças de segurança em tempo real e com operação 24x7;

11.2.4. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

11.2.5. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;

11.2.6. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

11.2.7. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

11.2.8. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

11.2.9. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;

11.2.10. Deve permitir operação em modo Mesh;

11.2.11. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

11.2.12. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

11.2.13. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

11.2.14. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);

11.2.15. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;

11.2.16. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;

11.2.17. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

11.2.18. Deve possuir indicadores luminosos (LED) para indicação de status;

12.0. GERÊNCIA CENTRALIZADA DE APS WIFI

12.0.1. A solução de gerência de wifi deve permitir o controle de todo o parque, em uma única console;

12.0.2. Deve permitir a autenticação de gerência via logins criados localmente, bem como se utilizar de bases externas: AD e radius;

12.0.3. Deve ser ofertada com todas as licenças necessárias para a gestão do parque: controladoras e APs. Além de suportar todos os recursos de wifi descritos nesse texto;

12.0.4. Deve permitir visualizar os APs conectados a cada controladora, caso se trate de um cenário distribuído;

12.0.5. Deve permitir a identificação de APs Rogue na console;

12.0.6. Deve listar todos os usuários de equipamentos conectados à rede wifi, em uma única tela e também por AP;

12.0.7. De dentro da console, deve permitir renomear os APs, realizar reboot, upgrade, definir profile, login e senha para acesso remoto aos APs e, por fim, obter informações adicionais como status, mac-address e quando se registrou à controladora/gerência;

12.0.8. Deve informar o status de cada AP: online, offine, não autorizado etc;

12.0.9. Deve permitir a adição de novos APs;

12.0.10. Deve mostrar, de forma detalhada, informações sobre cada usuário e/ou equipamento conectado à rede wireless: SSID, AP, IP do equipamento, mac-address, canal, banda, relação SNR, quando se associou, fabricante, OS e taxa de transferência;

12.0.11. Deve informar, em gráficos de forma temporal: uptime do APs, clientes ao longo do tempo, volume de clientes por AP, interferências e volume de clientes por frequência;

12.0.12. Deve permitir o posicionamento dos APs ou controladoras em mapa (Google ou similar) e também o upload de mapas customizados;

12.0.13. Por meio da gerência centralizada deve prover profiles para configurações diversas no ambiente wireless;

12.0.14. Deve suportar a configuração de profiles de AP: autenticação nas antenas para gestão, balanceamento de por AP e frequência, customização dos rádios, perfis de WIDS, country code, SSIDs a serem divulgados, canais, potência, tamanho do canal, dentre outras configurações;

12.0.15. Deve permitir a criação de SSIDS e grupos de SSIDs, informando: nome, modo de funcionamento, IP e máscara, DHCP server e relay, nome do SSID, agendamento, supressão de broadcast, pooling de vlans, quarentena, profile de QoS;

12.0.16. Deve permitir a criação de vários profiles de WIDS, contemplando as seguintes configurações: modo de funcionamento do sensor e tipos de ataque;

12.0.17. Deve considerar os seguintes ataques: aslead attack, association frame flooding, authentication frame flooding, broadcsting deauthentication, null SSID probe response, invalid MAC OUI e long duration attack.

13. SOLUÇÃO DE WEB APPLICATION FIREWALL VIRTUALIZADA

13.1. Funcionalidades Gerais:

13.1.1. A solução deve ser configurada em alta disponibilidade, ativo-ativo ou em cluster;

13.1.2. Cada solução virtualizada softwares específicos, destinados a finalidade de Firewall de Aplicação Web (WAF –Web Application Firewall), bem como as licenças necessárias para o seu funcionamento e proteção de servidores e aplicações Web;

13.1.3. A implantação da solução deverá ser planejada previamente em conjunto com a CONTRATANTE, onde deverão ser definidos todos os passos necessários para a instalação, incluindo o cronograma de implantação, planos de testes e homologação da solução;

13.1.4. Throughput mínimo para HTTP de 500 Mbps;

13.1.5. Suporte a pelo menos 10 interfaces de rede;

13.1.6. Suporte mínimo a pelo menos 2 vCPUs;

13.1.7. A solução deve oferecer suporte pelo menos aos seguintes Hypervisor: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox e KVM.

13.2. Funcionalidades de Rede

13.2.1. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo e Inline Transparente (Bridge)

13.2.2. A solução deve ser capaz de ser implementada com protocolo WCCP

13.2.3. Suportar VLANs no padrão IEEE 802.1q.

13.2.4. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs).

13.2.5. A solução deve suportar roteamento por política (policy route)

13.3. Funcionalidades de Gerência

13.3.1. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH.

13.3.2. Deve possuir administração baseada em interface web HTTP

13.3.3. Deve possuir administração baseada em interface de linha de comando via Telnet

13.3.4. Possuir auto complementação de comandos na CLI

13.3.5. Possuir ajuda contextual na CLI

13.3.6. A solução deve possuir um Dashboard com informações sobre o sistema (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware)

13.3.7. Deverá ser possível visualizar através da interface gráfica de gerencia informações de licenças, assinaturas e contrato de suporte

13.3.8. A solução ofertada deverá possuir acesso à linha de comando CLI via interface gráfica de gerencia

13.3.9. Deve prover, na interface de gerencia, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões.

13.3.10. Deve ser possível visualizar na interface de gerencia as informações de consumo de memória

13.3.11. Deverá possuir ferramenta, na interface gráfica de gerencia (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados

13.3.12. Deve prover as seguintes informações, na interface de gráfica de gerencia: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema

13.3.13. Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema

13.3.14. Possuir um painel de visualização com informações das interfaces de rede do sistema

13.3.15. A configuração de administração da solução deve possibilitar a utilização de perfis.

13.3.16. Deve ser possível executar e restaurar backup via interface Web (GUI)

13.3.17. Deve ter a opção para criptografar o backup utilizando algoritmo AES 128-bit ou superior

13.3.18. Deve ser possível executar e restaurar backup utilizando-se FTP

13.3.19. Deve ser possível executar e restaurar backup utilizando-se SFTP e TFTP

13.3.20. Deve ser possível antes de aplicar uma nova versão de firmware testar o mesmo em memória RAM sem instalação em disco

13.3.21. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal

13.3.22. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3

13.3.23. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog

13.3.24. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG

13.3.25. Ter a capacidade de armazenar logs em appliance remoto

13.3.26. A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias.

13.3.27. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web

13.3.28. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem , o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem.

13.3.29. Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário.

13.3.30. Deve ter suporte a RESTful API para gerenciamento de configurações

13.4. Funcionalidades de Autenticação

13.4.1. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS

13.4.2. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos

13.4.3. A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais

13.4.4. Deve possuir base local para armazenamento e autenticação contas de usuários.

13.4.5. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS

13.4.6. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM

13.4.7. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação

13.4.8. Deve suportar CAPTCHA e Real Browser Enforcement (RBE)

13.4.9. Deve suportar autenticação de duplo fator

13.5. Itens Regulatórios e Certificações

13.5.1. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10

13.5.2. O equipamento deve possuir certificação FCC Class A part 15

13.5.3. O equipamento deve possuir certificação C-Tick

13.5.4. O equipamento deve possuir certificação VCCI

13.5.5. O equipamento deve possuir certificação CE

13.5.6. O equipamento deve possuir certificação UL/cUL

13.5.7. O equipamento deve possuir certificação CB

13.6. Funcionalidades de Web Application Firewall

13.6.1. Deve ter suporte nativo de HTTP/2

13.6.2. Deve suportar tradução de HTTP/2 a HTTP 1.1

13.6.3. Deve suportar interoperabilidade com OpenAPI 3.0

13.6.4. Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de virus e IP reputation, atualizado de forma automática

13.6.5. A solução deve permitir escolher entre usar o banco de dados completo ou apenas uma base de dados contendo vírus mais recentes e perigosos

13.6.6. Deve ter algoritmos para detenção de ameaças avançadas baseados em aprendizagem de máquina com inteligência artificial (AI)

13.6.7. Deverá minimizar a ocorrência de Falsos Positivos e falsos negativos utilizando Inteligência Artificial

13.6.8. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários e o que se espera de cada campo

13.6.9. O perfil aprendido de forma automatizada pode ser ajustado e editado

13.6.10. Ter a capacidade de criação de assinaturas de ataque customizáveis

13.6.11. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol

13.6.12. Ter a capacidade de proteção para ataques do tipo Botnet

13.6.13. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST)

13.6.14. A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta

13.6.15. Deve suportar detecção a ataques de Clickjacking

13.6.16. Deve suportar detecção a ataques de alteração de cookie

13.6.17. Identificar e prevenir ataques do tipo Credit Cart Theft

13.6.18. Identificar e prevenir ataques Cross Site Request Forgery (CSRF)

13.6.19. A solução deverá possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS)

13.6.20. Deve possuir proteção contra ataques de Denial of Service (DoS);

13.6.21. Ter a capacidade de proteção para ataques do tipo HTTP header overflow

13.6.22. Ter a capacidade de proteção para ataques do tipo Local File inclusion (FLI)

13.6.23. Ter a capacidade de proteção para ataques do tipo Man-in-the0middle (MITM)

13.6.24. Ter a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI)

13.6.25. Ter a capacidade de proteção para ataques do tipo Server Information Leakage

13.6.26. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);

13.6.27. Ter a capacidade de proteção para ataques do tipo Malformed XML

13.6.28. Identificar e prevenir ataques do tipo Low-rate DoS

13.6.29. Prevenção contra Slow POST attack

13.6.30. Proteger contra ataques Slowloris

13.6.31. Ter a capacidade de proteção para ataques do tipo SYN flood

13.6.32. Ter a capacidade de proteção para ataques do tipo Forms Tampering

13.6.33. A solução deverá possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido

13.6.34. Ter a capacidade de proteção para ataques do tipo Directory Traversal

13.6.35. Ter a capacidade de proteção do tipo Access Rate Control

13.6.36. Reconhecer e remediar Zero Day Attacks

13.6.37. Ter a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold

13.6.38. Permitir configurar regras de bloqueio a métodos HTTP indesejados

13.6.39. Permitir que sejam configuradas regras de limite de upload por tamanho de arquivo

13.6.40. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país.

13.6.41. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado

13.6.42. Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem

13.6.43. Permitir a liberação temporária ou definitiva (allow list) de endereços IP bloqueados por terem originados ataques detectados pela solução.

13.6.44. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation

13.6.45. Ter a capacidade de conectar-se a uma base de dados na Internet para validar que as credenciais que usam os usuários para acessar a algum sistema não sejam credenciais roubadas.

13.6.46. Ter a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP

13.6.47. Ter a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha

13.6.48. Ter a funcionalidade de antivírus integrada para inspeção de tráfego e arquivos, sem a necessidade de instalação de outro equipamento

13.6.49. Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade.

13.6.50. Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia

13.6.51. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego

13.6.52. Para SSL/TLS offload suportar no mínimo SSL 3.0, TLS 1.0, 1.1 e 1.2

13.6.53. A solução deve ter a capacidade de armazenar certificados digitais de CA's.

13.6.54. A solução deve ser capaz de gerar CSR para ser assinado por uma CA.

13.6.55. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL)

13.6.56. A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões.

13.6.57. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente.

13.6.58. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores

13.6.59. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location

13.6.60. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessados para prevenir ataques como cross-site request forgery (CSRF).

13.6.61. A solução deve ter a capacidade de definir restrições a métodos HTTP

13.6.62. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos.

13.6.63. Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares

13.6.64. A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades para diagnostico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows

13.6.65. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros

13.6.66. Deve permitir agendar a verificação de vulnerabilidades

13.6.67. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML

13.6.68. Suportar redirecionamento e reescrita de requisições e respostas HTTP

13.6.69. Permitir redirecionar requisições HTTP para HTTPS

13.6.70. Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP

13.6.71. Permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP

13.6.72. Permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP

13.6.73. Permitir redirecionar requisições para outro web site

13.6.74. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP

13.6.75. Permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web

13.6.76. Permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web

13.6.77. Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso.

13.6.78. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit).

13.6.79. A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação

13.6.80. Possuir capacidade de caching para aceleração web

13.6.81. A solução deve ser capaz de submeter arquivos para solução de sandboxing do mesmo fabricante, através de uma política de restrição de carregamento de arquivo.

13.6.82. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.

13.7. Funcionalidades de Balanceamento de Carga

13.7.1. A solução deve incluir funcionalidade de balanceamento de carga entre servidores web

13.7.2. Deve ter a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS

13.7.3. Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web

13.7.4. A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários

13.7.5. Suportar algoritmo Round Robind para balanceamento de carga de servidores

13.7.6. Suportar algoritmo Weighted Round Robind para balanceamento de carga de servidores

13.7.7. Suportar algoritmo Least Connections para balanceamento de carga de servidores

13.7.8. A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido.

13.7.9. Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool.

13.7.10. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool

13.7.11. Permitir teste de disponibilidade de servidor web através do método TCP

13.7.12. Permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping)

13.7.13. Permitir teste de disponibilidade de servidor web através do método TCP Half Open

13.7.14. Permitir teste de disponibilidade de servidor web através do método TCP SSL

13.7.15. Permitir teste de disponibilidade de servidor web através do método HTTP

13.7.16. Permitir teste de disponibilidade de servidor web através do método HTTPS

13.7.17. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada

13.7.18. Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST

13.7.19. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado

13.7.20. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host"

13.7.21. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "URL"

13.7.22. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Parâmetro HTTP"

13.7.23. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Referer"

13.7.24. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Endereço IP de Origem"

13.7.25. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cabeçalho".

13.7.26. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cookie"

13.7.27. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Valor de campo do Certificado X509"

13.7.28. Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução.

13.7.29. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem

13.7.30. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP

13.7.31. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada

13.7.32. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite

13.7.33. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica)

13.7.34. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie

13.7.35. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente

13.7.36. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID

13.7.37. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID

13.7.38. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID

13.7.39. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL

13.8. SERVIÇOS DA SOLUÇÃO DE WEB APPLICATION FIREWALL – WAF

13.8.1. A implantação, configuração, gerenciamento, monitoramento dos serviços ofertados e manutenção e suporte da solução deverão ser realizados pela CONTRATADA.

13.8.2. É de responsabilidade da CONTRATADA todas as despesas com materiais, mão-de-obra, transportes, hospedagem, equipamentos, máquinas, impostos, seguros, taxas, tributos, incidências fiscais, trabalhistas, previdenciárias, salários, custos diretos e indiretos, encargos sociais e contribuições de qualquer natureza ou espécie, necessários à perfeita execução do objeto.

13.8.3. Quaisquer atualizações dos softwares das soluções deverão ser realizadas sem interrupções dos serviços WAF.

13.8.4. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de primeiro, segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente.

13.8.5. Entende-se por suporte técnico, mas não se limitando a, toda ação necessária da CONTRATADA para a normalização dos serviços WAF, solicitações da CONTRATANTE para a realização de configurações no ambiente WAF, criação e exclusão de regras e políticas de segurança entre outras que se fizerem necessárias na solução.

13.8.6. Em situações que forem identificadas como origem do incidente falhas nos links de comunicação e estes serem causados por contratos da CONTRATANTE com outras empresas, a CONTRATANTE deverá realizar o acionamento e acompanhamento do suporte técnico da referida empresa fornecedora do link afetado, para que esta realize a normalização dos seus serviços.

13.8.7. Todos os chamados, sejam abertos pela CONTRATANTE ou pela CONTRATADA de forma proativa e/ou reativa, deverão ser registrados em ferramenta para este fim, a qual deverá possibilitar a extração das informações de acordo com os relatórios exigidos mensalmente.

13.8.8. Os chamados abertos pelo CONTRATANTE serão referentes às atividades sob responsabilidade da CONTRATADA, englobando: instalação, configuração, recuperação, alteração e remoção de equipamentos, configurações na solução WAF, endereçamento IP, SNMP, organização e atualização da gerência e considerando-se todos os serviços contratados de maneira a assegurar a integridade, a qualidade e desempenho dos serviços dentro dos limites estabelecidos.

13.8.9. A CONTRATADA deverá manter atualizados no seu sistema de chamados as informações e status de andamento no atendimento dos incidentes/requisições.

13.8.10. Eventuais paradas na solução WAF, em qualquer nível, ou qualquer outra parada de responsabilidade da CONTRATADA, deverá ser comunicada tempestivamente a CONTRATANTE através de e-mail ou telefone(s) que possam garantir contato imediato a ser(em) informado(s) pela CONTRATANTE.

13.8.11. Todas as interrupções programadas deverão ser comunicadas ao CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis, e deverão ser realizadas preferencialmente aos domingos e feriados, ou em data e horário pré-definidos pelo CONTRATANTE, de acordo com o fuso horário da localidade onde ocorrerá a interrupção. As paradas programadas deverão ser autorizadas pelo CONTRATANTE antes de sua execução.

13.8.12. O CONTRATANTE poderá solicitar de acordo com suas necessidades, a qualquer tempo, alteração nas configurações da solução WAF.

13.8.13. O CONTRATANTE poderá solicitar, a qualquer tempo, os dados e demais informações armazenadas pela CONTRATADA em seu ambiente de gerência, relativos ao projeto do CONTRATANTE.

13.8.14. Os dados e informações armazenados poderão ser solicitados pelo CONTRATANTE, a qualquer tempo à CONTRATADA que deverá disponibilizá-los no prazo máximo de 5 (cinco) dias úteis, em meio a ser definido pela CONTRATANTE e/ou na base de dados da solução de gerência (carga dos dados extraídos e removidos).

13.9. MONITORAMENTO SOC

13.9.1. A CONTRATADA deverá realizar o monitoramento de toda a solução WAF, fornecida, atuando de forma proativa e reativa a eventos que possam causar impactos ou indisponibilidade na prestação dos serviços contratados.

13.9.2. A ferramenta utilizada para o gerenciamento deverá possibilitar o acompanhamento do desempenho da solução WAF, fornecendo no mínimo as seguintes opções:

13.9.2.1. Possibilitar visualizar os percentuais de ocupação de CPU e memória da solução de serviços WAF com os valores médios e de pico dos últimos 30 (trinta) dias, com possibilidade de visualização por dia e/ou período escolhido.

13.9.2.2. Deve permitir a elaboração de relatórios dos fluxos de comunicação em que deve ser possível verificar IP de origem e destino, protocolo da camada de transporte, porta de origem e destino da camada de transporte.

13.10. GERAL

13.10.1. A CONTRATADA deverá disponibilizar uma central única de atendimento, em tempo integral, operando em regime 24 horas por dia, 7 dias por semana, durante toda a vigência do contrato, a qual será acionada através de um número nacional único e não tarifado, ou um portal na internet, para abertura de chamados de suporte técnico e acompanhamento dos níveis de serviços prestados, com acesso restrito através de usuário/senha eletrônica;

13.10.2. A CONTRATANTE deverá disponibilizar acesso seguro ao ambiente para a CONTRATADA objetivando a realização do serviço de solução WAF;

13.10.3. Todos os recursos, mas não limitado há, de softwares e equipamentos necessários para realização do acesso seguro deverão ser de responsabilidade da CONTRATANTE;

13.10.4. Será permitida a subcontratação dos serviços de instalação e manutenção presencial (on-site) dos equipamentos, por se caracterizarem como acessórios ao serviço principal da solução de Web Application Firewall WAF VIRTUALIZADO;

13.10.5. Não será permitida a subcontratação do serviço de gerenciamento e monitoramento da solução;

14. ESPECIFICAÇÕES MÍNIMAS PARA O SERVIÇO DE ANÁLISE DE VULNERABILIDADE – WEB

14.1. O serviço deve ser capaz de verificar a existência de vulnerabilidades no ambiente alvo da CONTRATANTE, visando identificar possíveis brechas de segurança da informação.

14.2. Deverá verificar até 100 (cem) URL de Internet, a serem informadas pela CONTRATANTE após a assinatura do contrato;

14.3. O serviço deve ser capaz de realizar varreduras de vulnerabilidades específicas do ambiente alvo contratado incluindo a identificação das vulnerabilidades apresentadas no projeto do Owasp Top 10, como, por exemplo, Injection flaws (SQL injection etc.), cross-site scripting, command injection, directory traversal, buffer overflow, insecure cryptografic storage e improper error handling;

14.4. O Serviço deve utilizar como base metodológica para análise de vulnerabilidades partes pertinentes das metodologias OSSTMMv3, OWASPv4 quanto a identificação de vulnerabilidades de segurança em aplicações, sistemas operacionais e serviços ativos dentro das seguintes etapas:

14.4.1. Planejamento

14.4.2. Descoberta de Alvos e Serviços

14.4.3. Identificação de Vulnerabilidades

14.4.4. Validação das Vulnerabilidades

14.4.5. Relatório

14.4.6. Reteste

14.5. O serviço deve compreender as seguintes atividades no processo:

14.5.1. Análise de Vulnerabilidades em infraestrutura Web: Identificação dos serviços e tecnologias e as vulnerabilidades associadas no ambiente alvo.

14.5.2. Gerenciamento do Cronograma do Projeto (data de início; data de término, responsáveis, entregáveis);

14.5.3. Status Report de evolução do Projeto;

14.5.4. Gerenciamento do plano de ação de correções de vulnerabilidades;

14.5.5. Desenvolvimento e apresentação do relatório executivo de vulnerabilidades;

14.5.6. Garantir cumprimento dos entregáveis previstos;

14.6. O serviço de análise de vulnerabilidades deve contemplar a seguinte documentação:

14.6.1. Relatório Técnico Detalhado: Incluindo sistemas afetados, descrição, classificação do risco, remediação e referência.

14.6.2. Relatório Técnico Gerencial: Incluindo sistemas afetados, título, descrição e status.

14.6.3. Relatório Técnico Executivo: Consolidação das vulnerabilidades com uma visão executiva de riscos associados aos alvos/ambiente.

14.7. Para a prestação do serviço, a solução a ser utilizada devera possuir as características a saber:

14.7.1. O gerenciamento da solução deve ser 100% em nuvem;

14.7.2. A solução deve prover no mínimo 99.95% de disponibilidade no nível de serviço;

14.7.3. A solução deve ser licenciada de modo a realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

14.7.4. Deve possibilitar, por meio da console, no mínimo 3 (três) métodos de escaneamento:

14.7.4.1. Scan ativo;

14.7.4.2. Scan com uso de agentes;

14.7.4.3. Scan passivo;

14.7.4.4. Deve ser capaz de identificar no mínimo 53.000 CVE´S;

14.7.5. A solução deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades diferente do padrão CVSS;

14.7.6. Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial;

14.7.7. O Algoritmo de priorização deve considerar no mínimo 100.000 vulnerabilidades distintas para realizar o cálculo do score da vulnerabilidade;

14.7.8. Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades;

14.7.9. A solução deve ser capaz de aplicar algoritmos de inteligência artificial (Machine learning) para analisar mais de 130 fontes de dados relacionadas a vulnerabilidades;

14.7.10. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

14.7.10.1. CVSSv3 Impact Score;

14.7.10.2. Idade da Vulnerabilidade;

14.7.10.3. Se existe ameaça ou exploit que explore a vulnerabilidade;

14.7.10.4. Número de produtos afetados pela vulnerabilidade;

14.7.10.5. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;

14.7.10.6. Lista de todas as fontes (canais de mídia social, dark web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade;

14.7.11. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades, incluindo feeds de inteligência de ameaças ao vivo;

14.7.12. A solução deve possuir conectores para a seguintes plataformas:

14.7.12.1. Amazon Web Service (AWS);

14.7.12.2. Microsoft Azure;

14.7.12.3. Google Cloud Platform;

14.7.12.4. Qualys Assets;

14.7.13. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

14.7.14. A solução deverá capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

14.7.15. A plataforma deverá avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

14.7.16. Deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;

14.7.17. Deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

14.7.18. Deve possui modelos (templates) prontos de varreduras entre simples e extensos;

14.7.19. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

14.7.19.1. Cookies, Headers, Formulários e Links;

14.7.19.2. Nomes e valores de parâmetros da aplicação;

14.7.19.3. Elementos JSON e XML;

14.7.19.4. Elementos DOM;

14.7.20. Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

14.7.21. Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

14.7.22. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

14.7.23. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

14.7.24. Deve ser capaz de instituir no mínimo os seguintes limites:

14.7.24.1. Número máximo de URLs para crawl e navegação;

14.7.24.2. Número máximo de diretórios para varreduras;

14.7.24.3. Número máximo de elementos DOM;

14.7.24.4. Tamanho máximo de respostas;

14.7.24.5. Limite de requisições de redirecionamentos;

14.7.24.6. Tempo máximo para a varredura;

14.7.24.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

14.7.24.8. Número máximo de requisições HTTP por segundo;

14.7.25. A solução deve ser capaz de detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

14.7.25.1. Limite em segundos para timeout de requisições de rede;

14.7.25.2. Número máximo de timeouts antes que a varredura seja abortada;

14.7.25.3. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

14.7.26. Deve ser capaz de enviar notificações através de no mínimo E-mail e SMS;

14.7.27. Deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

14.7.28. Deverá avaliar sistemas web utilizando protocolos HTTP e HTTPs;

14.7.29. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

14.7.30. Deverá ser compatível com avaliação de web services REST e SOAP;

14.7.31. Deverá suportar no mínimo os seguintes esquemas de autenticação:

14.7.31.1. Autenticação básica (digest);

14.7.31.2. NTLM;

14.7.31.3. Form de login;

14.7.31.4. Autenticação de Cookies;

14.7.31.5. Autenticação através de Selenium;

14.7.32. Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário;

14.7.33. Deve ser capaz de customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

14.7.34. Deve ser capaz de exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

14.7.35. Deve ser capaz de exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

14.7.36. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

14.7.37. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

14.7.38. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc.), deve evidenciar nos detalhes do evento encontrado:

14.7.38.1. Payload injetado;

14.7.38.2. Evidência em forma de resposta da aplicação;

14.7.38.3. Detalhes da requisição HTTP;

14.7.38.4. Detalhes da resposta HTTP;

14.7.38.5. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

14.7.39. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

14.7.40. A solução deve possuir suporte a varreduras de componentes para no mínimo: WordpPess, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat,
Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

15. DOCUMENTAÇÕES ENTREGÁVEIS

15.1. Mensalmente deverão ser entregues os seguintes relatórios ou disponibilizados via portal web:

15.1.1. Os registros dos chamados atendidos no período de prestação de serviço contendo todas as informações relativas aos chamados resolvidos, como: data de abertura, tempo para o atendimento, tempo de resolução, data de resolução, identificação do elemento afetado, descrição detalhada da resolução do chamado, nível de prioridade e percentual (%) de atendimento e de resolução do tempo definido no SLA.

15.1.2. Relatório de chamados com status aberto no período de prestação de serviço contendo informações como data, hora, identificação do elemento (circuito ou equipamento).

15.1.3. Relatório com as reincidências de problemas.

15.1.4. Somatórios dos minutos de interrupção de cada circuito.

15.1.5. Cálculos de percentuais de disponibilidade por localidade, correspondente ao período de faturamento com informações diária, semanal e mensal. Devem conter as informações referentes ao desempenho e à utilização dos recursos da rede.

15.1.6. Relatórios de Tráfego: Apresentam o tráfego de todos os circuitos, com suas séries históricas, fornecendo subsídios para analisar o desempenho e as tendências de aproveitamento dos recursos da rede. Devem demonstrar informações da banda utilizada e do volume de tráfego.

15.1.7. Relatório de disponibilidade da solução de web application firewall – WAF, observando item de SLA.

15.1.8. O formato dos relatórios será definido em conjunto

15.1.9. entre a CONTRATANTE e a CONTRATADA quando da implantação da solução de gerenciamento.

15.1.10. No decorrer da execução do contrato o CONTRATANTE poderá solicitar novos tipos de relatórios que deverão ser disponibilizados em até 72 horas.

16. ESPECIFICAÇÕES MÍNIMAS PARA A GERÊNCIA DE REDES E SERVIÇOS

16.1. Requisitos mínimos e obrigatórios do serviço de gerência de rede e serviços:

16.1.1. A CONTRATADA deverá prover Solução de Gerência da Rede que contemple os módulos de gerência de falhas, desempenho, disponibilidade, capacity planning, relatórios, tickets e de nível de serviço:

a) A Solução de Gerência da Rede deverá disponibilizar a visualização de informações on-line (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

b) Em caso de formação de consórcio deverá ser provida uma única solução de Gerência de Rede.

16.1.2. A Solução de Gerência da Rede da CONTRATADA deverá atuar de forma pró-ativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano.

16.2. Requisitos da Solução de Gerência de Rede:

16.2.1. A Solução de Gerência da Rede:

16.2.1.1. A solução fornecida deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento;

16.2.1.2. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto não serão aceitos soluções que possuem acessos segmentados aos módulos;

16.2.1.3. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados.

16.2.1.4. Deverá permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc;

16.2.1.5. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente.

16.2.1.6. A Solução de Gerência da Rede deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

16.2.1.7. Os perfis deverão prever configurações em níveis de alertas, equipamentos, interfaces, aplicações, funcionalidades de monitoração, capacity planning, inventário, etc;

16.2.1.8. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação de clients específicos, portanto não serão aceitas soluções que não sejam nativas em WEB ou que requeiram a instalação de agentes ou plugins nos desktops dos colaboradores da CONTRATANTE;

16.2.1.9. O acesso deverá ser via web padrão HTTP e suportar a HTTPS, e em português, portanto não serão aceitas soluções que não possuam toda a sua estrutura em português;

16.2.1.10. A Solução de Gerência da Rede deverá ser compatível para acesso através de smartphones e tablets, portanto não serão aceitas soluções que não possuam essa compatibilidade;

16.2.1.11. A Solução de Gerência da Rede deverá ser escalável, mas transparente para a CONTRATANTE em termos de console única;

16.2.1.12. A Solução de Gerência da Rede deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari;

16.2.1.13. Deverá permitir a exportação das informações para relatórios em formatos comerciais;

16.2.1.14. A Solução de Gerência da Rede deverá gerar alertas quando os thresholds “limites” configurados para um componente monitorado são excedidos (ex., utilização de CPU, memória, interfaces, volume de erros, tempo de resposta de serviços);

16.2.2. A Solução de Gerência da Rede deverá fornecer, através do portal, visualização de informações on-line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos elementos monitorados:

a) Topologia da rede, incluindo os roteadores CPE e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que os mesmos sofrerem alterações;

b) Alarmes e eventos ocorridos na rede com informações de data, hora e duração de ocorrência e identificação dos recursos gerenciados;

c) Consumo de banda dos enlaces (entrada e saída) separados por dia e mês;

d) Consumo de banda por classe de serviço separados por dia e mês;

e) Ocupação de memória e CPU dos roteadores CPE;

f) Retardo dos enlaces separados por dia e mês;

g) Perda de pacotes (descarte) no sentido IN e OUT em %;

h) Taxa de erros em erros por segundo;

i) Latência em milissegundos;

j) A Solução de Gerência de Rede de possuir gráficos de Capacity Planning que permita criar uma série de cenários para projeções de tendências de um determinado recurso;

k) A Solução de Gerência da Rede deverá permitir a apresentação de indicadores que reflitam o nível de SLA (Service Level Agreement) e SLM (Service Level Management) dos serviços contratados;

l) Backup de configuração dos elementos gerenciados, alarmes para alterações realizadas, relatório de mudanças;

m) Inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:

i.1) Enlace: designação, tecnologia e nível de serviço;

i.2) Roteador CPE: fabricante e modelo e configuração física (interfaces, memória, slots, dentre outros);

i.3) Endereçamento lógico: endereços IPs e máscaras;

n) A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados;

16.2.3. A Solução de Gerência da Rede deverá permitir a criação de Relatórios:

a) Permitir ser exportados conforme os principais métodos como: pdf, csv, pacote office;

b) Relatórios de desempenho sumarizado por período especifico;

c) Relatórios de desempenho classificados em uma visão TOP N. Ex.:

i. Top Roteadores % de utilização de CPU

ii. Top N Interfaces % de utilização

iii. Top N Interfaces com descartes

iv. Top N Interfaces com eventos de Latência

d) Relatórios de disponibilidade com períodos específicos;

e) Dashboards relacionando falhas, desempenho, capacity e disponibilidade;

f) Dashboards executivos com visão sumarizadas de indicadores operacionais (Pro atividade, Taxa de Reincidência, Reparos no Prazo e Taxa de Falha);

16.2.4. A Solução de Gerência da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados.

16.2.5. A Solução de Gerência da Rede deverá armazenar os dados por um período de 6 (seis) meses.

17. PADRÃO DE DESEMPENHO:

17.1. A CONTRATADA deverá assegurar os seguintes padrões de desempenho para o serviço:

17.1.1. Deverá ser garantida uma perda de pacotes fim a fim (end-to-end), que consiste na taxa de sucesso na transmissão de pacotes IP que entra (incoming) numa ponta, e sai (outgoing) em outra ponta da nuvem da CONTRATADA, deverá ser de no máximo 2%.

17.1.2. Deverá ser garantida disponibilidade, que consiste no percentual de tempo no qual a nuvem da CONTRATADA está operacional em um período de tempo, de no mínimo 99% no concentrador e 98% nos remotos.

17.1.3. Entende-se por disponibilidade, a liberação dos links de comunicações por parte da CONTRATADA, após instalação, configuração e constatação do perfeito funcionamento dos mesmos conectados à Rede Corporativa da TJAC e acesso à Internet.

17.1.4. Qualquer paralisação será considerada como indisponibilidade.

17.1.5. A CONTRATADA deverá fornecer relatórios gráficos diários, mensais e anuais do tipo MRTG para quaisquer das interfaces LAN e WAN dos equipamentos fornecidos, através de página Web, mostrando os níveis de desempenho e de utilização dos links (velocidade real da porta x tempo), valores médios, máximos, mínimos, etc., de sorte a proporcionar à TJAC ferramentas de avaliação técnica para adoção de ações preventivas ou corretivas quando requeridas.

18. ENDEREÇOS E VELOCIDADES:

18.1. As velocidades estão de acordo com a resolução 211/2015 do CNJ Art. 24 Item VI, onde exige 2 (dois) Links de comunicação do órgão com a internet, mas com operadoras distintas para o acesso à rede de dados, com o máximo de comprometimento de banda de 80%, como é demonstrado nos GRUPO 1 e GRUPO 2, do Termo de Referência. Visa ainda atender a Resolução CNJ 370/2021 que não anula as ações/iniciativas do TJAC para atender os requisitos mínimos do nivelamento tecnológico da infraestrutura de TIC, conforme recomendado na Resolução 211/2015 no Art. 24, item VI, conforme deliberado na reunião com CNJ, em 10/03/2021, constante no SEI 0000550-59.2021.0000 item 18 (0944980):

"Com A Revogação da Res. CNJ nº 211/2015 e a publicação da Res. CNJ nº 370/2021 novas estratégias foram traçadas. Entendemos que pelo bem da Administração Pública, as estratégias passadas se tornaram boas práticas que merecem ser continuadas ou mesmo aperfeiçoadas."

18.2. A interligação do Tribunal de Justiça do Estado do Acre com a Internet deverá ser através de Link dedicado ponto-a-ponto e, as CONTRATADAS deverão fornecer, no mínimo, 254 (duzentos e cinquenta e quatro) números IPs próprios/públicos e válidos na Internet para o ITEM 01 do GRUPO 1 e de, no mínimo, 254 (duzentos e cinquenta e quatro) números IPs próprios/públicos e válidos na Internet para o ITEM 01 do GRUPO 2.

18.3. Os endereços e velocidades respectivas estão descritas nos itens 01, 02 e 03 do GRUPO 1 e 01 e 02 do GRUPO 2.

19. NÍVEIS MÍNIMOS DE SERVIÇO (NMS) PARA SERVIÇOS DE REDE E INTERNET:

19.1. Para cada um dos itens do objeto, a prestação dos serviços deverá atender a Níveis Mínimos de Serviço (NMS), conforme as condições elencadas a seguir:

19.1.1. Os serviços de acesso à Internet deverão estar operacionais em um regime 24x7 e deverão atender a um Índice de Disponibilidade Mensal (IDM) de 99,35%.

19.1.2. O Índice de Disponibilidade Mensal (IDM) deverá ser calculado mensalmente por meio da seguinte fórmula:

IDM = [(Tm – Ti) / Tm] *100, onde:

IDM é o Índice de Disponibilidade Mensal do serviço, em por cento.

Tm é o tempo total mensal de operação, em minutos, no mês de faturamento.

Ti é o somatório dos períodos de indisponibilidade do serviço, em minutos, no mês de faturamento.

19.1.3. Além do Índice de Disponibilidade Mensal (IDM), deverá ser aferida métrica correspondente ao Percentual de Pacotes com Erros de Transmissão (PET), que, uma vez superada, deverá ser considerada como período de indisponibilidade do serviço:

a) A métrica Percentual de Pacotes com Erros de Transmissão (PET) se refere à relação existente entre a quantidade de pacotes transmitidos/recebidos com erro e quantidade de pacotes transmitidos/recebidos, em cada acesso contratado.

b) Para medição desse percentual, quando solicitada, a CONTRATADA deverá realizar aferições do percentual de pacotes com erros para cada enlace integrante do acesso contratado, através da monitoração das interfaces WAN contratadas. As aferições deverão ser feitas em cada interface, por sentido de tráfego (inbound/outbound), apresentadas em valores referentes a cada intervalo de 05 (cinco) minutos, sendo o limite aceitável de erros de até 1,0% (um e meio por cento) do total de pacotes trafegados em cada interface e sentido.

c) Para cada valor da taxa de erros por pacotes acima do limite permitido no subitem anterior, deverá ser computado período de indisponibilidade de 05 (cinco) minutos na fórmula do IDM.

19.1.4. Além dos dois indicadores anteriores, deverá ser aferida métrica correspondente ao Percentual de Descarte de Pacotes (PDP), que, uma vez superada, deverá ser considerada como período de indisponibilidade de serviço:

a) A métrica Percentual de Descarte de Pacotes (PDP) se refere a relação existente entre a quantidade de pacotes transmitidos/recebidos descartada para cada pacote transmitido/recebido, em cada acesso contratado.

b) Quando solicitada, a CONTRATADA deverá realizar aferições do percentual de descarte de pacotes para cada enlace integrante do acesso contratado, através da monitoração das interfaces dos roteadores de acesso e do backbone participante do enlace. As aferições serão feitas em cada interface, por sentido (inbound/outbound), apresentadas em valores referentes a cada intervalo de 05 (cinco) minutos, sendo o limite aceitável de descartes de até 2,0% (dois por cento) do total de pacotes trafegados em cada interface e sentido.

c) Serão desconsiderados os valores que ultrapassem este limite quando a CONTRATADA comprovar a utilização superior a 80% (oitenta por cento) da velocidade do respectivo enlace no mesmo intervalo.

d) Sempre que o percentual de descarte de pacotes for superior ao limite máximo permitido, será computado período de indisponibilidade de 05 (cinco) minutos na fórmula do IDM.

19.1.5. Sempre que duas aferições de PET e PDP estiverem acima do limite máximo permitido, desde que elas ocorram em uma mesma porta de comunicação e durantes os mesmos intervalos de tempo de um mesmo dia, somente deverá ser computado o período de indisponibilidade associada a uma delas.

19.1.6. Indisponibilidades serão consideradas quando ocorrer qualquer tipo de problema nos equipamentos, links de comunicação ou backbone da CONTRATADA, que impeça a transmissão ou recepção de pacotes nos serviços de acesso à Internet ou impactem no seu desempenho.

19.1.7. No caso de links físicos múltiplos, a indisponibilidade de qualquer um dos links será considerada indisponibilidade do serviço como um todo, caracterizada pela limitação de uso e consequente propagação dos efeitos da falha.

19.1.8. Não serão computadas no cálculo da disponibilidade mensal até 08 (oito) interrupções anuais do serviço, qualificadas como janelas de manutenção preventiva, provocadas pela CONTRATADA e previamente agendadas em comum acordo com o TJAC, com antecedência mínima de 07 (sete) dias úteis, desde que executadas fora do expediente do Tribunal.

19.1.9. A violação de qualquer nível de serviço só poderá ser desconsiderada pelo TJAC quando for decorrente de falha em algum equipamento de propriedade do Tribunal, decorrente de procedimentos operacionais por parte do Tribunal, por qualquer equipamento da contratada que não possa ser corrigida por inacessibilidade causada pelo Tribunal ou eventuais interrupções programadas, desde que previamente autorizadas pelo TJAC.

20. ACORDO DE NÍVEL DE SERVIÇOS (SLA) PARA SERVIÇOS DE SEGURANÇA

20.1. Não serão consideradas indisponibilidades as seguintes situações:

20.1.1. Paradas programadas pela CONTRATADA e aprovadas pelo CONTRATANTE.

20.1.2. Paradas ocasionadas por casos fortuitos ou de força maior, devidamente comprovados;

20.1.3. Paradas ocasionadas por responsabilidades de TERCEIROS ou da CONTRADA;

20.1.4. Parada parcial, ou total, de apenas um dos equipamentos da solução de WAF desde que o equipamento remanescente esteja operacional;

20.2. A contagem para a solução do problema se iniciará a partir do registro do incidente no sistema de chamados da CONTRATADA, sendo este registro realizado pelo CONTRATANTE ou pela própria empresa contratada.

20.3. DEFINIÇÕES DE PRIORIDADE

20.3.1. Cada chamado (requisição de serviço/incidente) registrado deverá ter uma prioridade definida. Esta prioridade define a ordem de tratamento dos chamados, bem como outras questões relativas ao atendimento do mesmo, como o tempo de resolução.

20.3.2. PRIORIDADE - É definida em função da relevância do chamado em relação ao negócio da organização. É dividida em:

20.3.2.1. Prioridade ALTA - Chamados motivados por incidentes e/ou requisições com comprometimento total e/ou parcial de funcionalidade da solução, seja para um sistema, ambiente. Não existem alternativas disponíveis para que os usuários possam realizar o trabalho. A interrupção do serviço pode resultar em queda de produtividade, comprometer os compromissos do CONTRATANTE com outras empresas e/ou o atendimento a clientes por parte do CONTRATANTE.

20.3.2.2. Prioridade MÉDIA - Chamados motivados por incidentes e/ou requisições com degradação de funcionalidade da solução, seja para um sistema, ambiente e/ou para uma localidade. Existe alternativa disponível para a solução, mesmo que precária, no entanto algumas tarefas podem ficar afetadas até que o problema seja resolvido, podendo resultar em redução de produtividade.

20.3.2.3. Prioridade BAIXA - Chamados motivados por incidentes e/ou requisições sem comprometimento de funcionalidade da solução, seja para um sistema, ambiente e/ou para uma localidade. Existe alternativa disponível para a solução, no entanto algumas tarefas podem ficar afetadas até que o problema seja resolvido, não resultando em redução de produtividade, ou em perda de arrecadação.

Prioridade	**Tempo de Atendimento (SLA)**
	Atendimento após abertura do chamado
Alta	4 horas
Média	8 horas
Baixa	12 horas

Prioridade	**Tempo de Solução (SLA)**
	Solução do chamado após o atendimento
Alta	12 horas
Média	18 horas

Baixa	24 horas

21. DA ENTREGA E DO RECEBIMENTO:

21.1. A Empresa contratada deverá entregar o objeto no prazo máximo de até 60 (SESSENTA) dias corridos, a contar da data do recebimento da ordem de serviço. Após este prazo, o fornecedor ficará sujeito a sanções por mora ou inadimplemento parcial ou total do contrato.

21.1.1. Em caso de necessidade de elaboração de projeto específico para viabilizar a infraestrutura necessária à prestação do serviço, o prazo de entrega do serviço poderá ser prorrogado por igual período mediante justificativa da contratada, a ser entregue antes de findar o prazo inicial.

21.2. O prazo de instalação poderá ser dilatado por igual período ao prazo original, desde devidamente justificado pela CONTRATADA e solicitada com 15 dias antes do prazo final para ativação dos serviços;

21.3. No caso de atrasos na ativação do serviço ocasionados por responsabilidade da CONTRATANTE não serão computados ao prazo de ativação do serviço, sem prejuízo a possibilidade de ampliação do prazo de ativação previsto no item 21.1;

21.2. No ato da entrega, os produtos (modems, roteadores, firewalls e equipamentos wifi e serviços virtualizados) serão previamente vistoriados e, se verificadas irregularidades, serão colocados à disposição da empresa contratada, que terá o prazo máximo de 10 (dez) dias para substituí-los, circunstância que não interromperá o prazo de execução contratual.

21.3. Em conformidade com os artigos 73 a 76 da Lei nº 8.666/93, o objeto deste contrato será recebido da seguinte forma:

21.3.1. **Provisoriamente**, no ato da entrega, para efeito de posterior verificação da conformidade dos equipamentos com as especificações deste Termo de Referência.

21.3.2. **Definitivamente**, em até 10 (dez) dias após o recebimento provisório, mediante atesto na nota fiscal/fatura, após a verificação da qualidade dos produtos e aceitação pelo fiscal deste instrumento convocatório.

21.3.3. Não serão admitidos para efeito de recebimento itens que estejam em desacordo ou conflitantes com quaisquer especificações prescritas neste Termo de Referência.

21.4. O recebimento do objeto desta contratação será condicionado à conferência, ao exame qualitativo e à aceitação final, obrigando-se a CONTRATADA a reparar, corrigir, substituir, no todo ou em parte, sanar os vícios, defeitos ou as incorreções porventura detectadas.

21.1. O recebimento dar-se-á por meio de **Termo de Aceite**, emitido pela Unidade de Tecnologia da Informação da CONTRATANTE, provisoriamente em até 5 (cinco) dias corridos, contados da ativação do mesmo e de forma definitiva em até 10 (dez) dias corridos do recebimento provisório, após verificado o perfeito estado de funcionamento e atendimento às características exigidas neste documento e anexos;

21.2. O faturamento de cada acesso terá início a partir da data da emissão do Termo de Aceite;

21.3. Em caso de falta de manifestação por parte da CONTRATANTE o serviço será automaticamente considerado aceito de forma automática após 15 (quinze) dias corridos da ativação dos serviços;

22. RESPONSABILIDADES DAS PARTES:

22.1. DA CONTRATANTE:

22.1.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA, para a instalação dos Links.

22.1.2. Fiscalizar o cumprimento das obrigações assumidas pela CONTRATANTE, inclusive quanto à continuidade da prestação dos serviços que ressalvados os casos de força maior, justificados e aceitos pelo Poder Judiciário, não deva ser interrompida.

22.1.3. Atestar o material entregue pela CONTRATADA, quanto ao critério de quantidade e qualidade.

22.1.4. Atestar os materiais recebidos, bem como sua nota fiscal/fatura.

22.1.5. Após atestar o recebimento do material, realizar pagamento uma vez que tenham sido cumpridos todos os critérios estabelecidos neste termo de referência.

22.1.6. Receber e conferir os materiais com base na autorização de empenho e no processo de contratação.

22.1.7. Fiscalizar, por meio da Diretoria de Tecnologia da Informação – DITEC a execução do objeto contratual.

22.1.8. Efetuar o pagamento do valor constante na nota fiscal/fatura, no prazo máximo de 15 (quinze) dias úteis, contados do recebimento da nota fiscal/fatura devidamente atestada.

22.1.9. Notificar o fornecedor registrado sobre eventuais atrasos na entrega dos materiais e/ou descumprimento de cláusulas previstas neste Termo de Referência, no Edital ou no contrato.

22.1.10. Aplicar ao fornecedor contratado as sanções administrativas regulamentares e contratuais cabíveis.

22.2. DA CONTRATADA:

22.2.1. Os Links serão instalados conforme a necessidade do Poder Judiciário, em estrita observância ao processo de modernização tecnológica e interligação das Unidades e Comarcas, da Capital e do Interior do Estado, mediante emissão de Ordem de Serviço.

22.2.2. É de responsabilidade da CONTRATADA o fornecimento dos modems e roteadores, bem como a sua configuração pré-estabelecida pela CONTRATANTE.

22.2.3. Cumprir integralmente todas as condições estabelecidas, sujeitando-se, inclusive, às penalidades pelo descumprimento de quaisquer de suas cláusulas.

22.2.4. Entregar os materiais e executar o serviço de instalação, nos prazos estabelecidos.

22.2.5. Em todo caso de devolução ou extravio dos materiais, responsabilizar-se pelo pagamento de fretes, carretos, seguros e tributos, se ocorrerem.

22.2.6. Pagar todos os tributos, contribuições fiscais e para fiscais que incidam ou venham incidir, direta ou indiretamente, sobre os materiais solicitados.

22.2.7. Entregar os materiais acondicionados em caixas e embalagens adequadas, com marca do fabricante e referência, a fim de evitar avarias e deterioração durante o transporte (exceto os materiais que incluem instalação).

22.2.8. Incluir, nos preços ofertados, todas as despesas de custo, seguro, frete, passagens, diárias, alimentação, montagem, instalação e testes dos equipamentos, encargos fiscais, comerciais, sociais e trabalhistas, ou de qualquer outra natureza.

22.2.9. Fornecer os materiais com observância dos demais encargos e responsabilidades cabíveis.

22.2.10. Prestar todos os esclarecimentos que lhe forem solicitados pelo Tribunal de Justiça do Estado do Acre, atendendo prontamente a todas as reclamações.

22.2.11. Comunicar imediatamente ao Tribunal de Justiça do Estado do Acre qualquer alteração ocorrida no endereço, conta bancária e outros julgados necessários para o recebimento de correspondência.

22.2.12. Indenizar terceiros e/ou o Tribunal de Justiça do Estado do Acre, mesmo em caso de ausência ou omissão de fiscalização de sua parte, por quaisquer danos ou prejuízos causados, devendo o fornecedor registrado adotar todas as medidas preventivas, com fiel observância às exigências das autoridades competentes e às disposições legais vigentes.

22.2.13. Solicitar do Tribunal de Justiça do Estado do Acre, em tempo hábil, quaisquer informações ou esclarecimentos que julgar necessários, que possam vir a comprometer a execução do objeto contratual.

22.2.14. Remover, às suas expensas, no prazo máximo de 30 dias corridos, contados do recibo da notificação, o material que, em virtude de sua rejeição, tiver sido substituído, sob pena de descarte ou reaproveitamento por parte da Administração.

22.2.15. Responder por quaisquer danos causados direta ou indiretamente ao TJAC, ou a terceiros, decorrentes de sua culpa ou dolo, na entrega do material, não excluindo ou reduzindo essa responsabilidade, mesmo que não haja fiscalização ou o acompanhamento do TJAC.

22.2.16. Disponibilizar acesso a portal WEB para retirada de faturas bem como desempenho dos Links fornecidos com as condições mínimas de ocupação de banda, acompanhamento de chamados.

23. GESTÃO E FISCALIZAÇÃO DOS SERVIÇOS:

23.1. Em consonância com o Decreto 9507/2018 e a disposição 2.6 do Anexo V da IN 05/2017 – SEGES/MP, a gestão e a fiscalização da execução dos contratos compreendem o conjunto de ações que objetivam:

I - aferir o cumprimento dos resultados estabelecidos pela contratada;

II - verificar a regularidade das obrigações previdenciárias, fiscais e trabalhistas; e

III - prestar apoio à instrução processual e ao encaminhamento da documentação pertinente para a formalização dos procedimentos relativos a repactuação, reajuste, alteração, reequilíbrio, prorrogação, pagamento, aplicação de sanções, extinção dos contratos, entre outras, com vistas a assegurar o cumprimento das cláusulas do contrato a solução de problemas relacionados ao objeto.

23.2. A gestão do contrato se dará da seguinte forma:

11.2.1. A Diretoria de Tecnologia da Informação - DITEC por meio de sua supervisão administrativa, é a Unidade organizacional responsável pela realização das atividades técnicas em telefonia, computação e internet do Tribunal, sendo desta forma a área de interveniência da execução do contrato, donde se tem hierarquicamente como:

a) Gestor do Contrato: Isaac Timoteo de Oliveira Junior
b) Fiscal do Contrato: Elson Correia de Oliveira Neto

23.3. A comunicação entre o Tribunal e a CONTRATADA se dará prioritariamente por e-mail, central informatizada de atendimento, quando disponível, e por telefone nas situações em que os meios de registro da demanda estiverem indisponíveis ou em situações emergenciais em que se pretenda resposta imediata.

23.4. Em caso de eventual irregularidade, inexecução ou desconformidade na execução do contrato, o agente fiscalizador notificará à Contratada, por escrito, estabelecendo prazo para adoção das providências necessárias para sanar as falhas apontadas.

23.5. Quando a contratada não produzir os resultados, ou não executar os serviços com a qualidade mínima exigida, poderão ocorrer descontos no pagamento devido, sem prejuízo das demais penalidades constantes do contrato.

23.6. O fiscal do contrato verificará o cumprimento das obrigações da contratada de manter todas as condições nas quais o contrato foi assinado durante todo o seu período de execução.

23.7. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da Contratada por quaisquer irregularidades, inexecuções ou desconformidades havidas na execução do objeto, aí incluídas imperfeições de natureza técnica ou aquelas provenientes de vício redibitório, como tal definido pela lei civil.

23.8. O Contratante reserva-se o direito de rejeitar, no todo ou em parte, o objeto da contratação, caso o mesmo afaste-se das especificações do Edital, seus anexos e da proposta da Contratada.

23.9. As decisões e providências que ultrapassem a competência do Fiscal do Contrato serão encaminhadas à autoridade competente da CONTRATANTE para adoção das medidas convenientes, consoante disposto no § 2ºdo art. 67, da Lei nº. 8.666/93.

23.10. Durante a execução do objeto, o fiscal deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

23.11. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, devem ser aplicadas as sanções à CONTRATADA de acordo com as regras previstas no ato convocatório.

23.12. Ao Gestor do contrato cabe a análise de reajuste; repactuação; reequilíbrio econômico-financeiro; incidentes relativos a pagamentos; de questões ligadas à documentação, ao controle dos prazos de vencimento e da prorrogação, apontando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

24. DOS REQUISITOS DE HABILITAÇÃO TÉCNICA:

24.1. Atestado ou declaração de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove, no mínimo, que a licitante tenha fornecimento, satisfatoriamente, 01 (um) Link Urbano (Internet) de 500 Mbits.

24.2. Ato de concessão/autorização para exploração do serviço objeto desta licitação.

24.3. Atestado de capacidade técnica ou certidão, no mínimo, expedido por pessoa jurídica de direito público ou privado, apresentado em papel timbrado da emitente que comprovem ter o licitante prestado serviços ou fornecidos produtos, de maneira satisfatória, compatíveis em características com o objeto desta licitação.

Atestado(s) ou declaração(ões) de capacidade técnica, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, comprovando fornecimento, por período não inferior a 1 (um) ano, de serviço de gestão de segurança de solução web application firewall (WAF), incluindo;

• Instalação;
• Licenciamento;
• Operação;
• Configuração;

Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.

Declaração e/ou Certidão comprovando de que a LICITANTE está autorizada, pelo fabricante da solução de web application firewall ofertada, a prestar serviço de segurança gerenciado;

Apresentação de profissional certificado em nível profissional em soluções de segurança do fabricante da solução de web application firewall ofertada;

Para fins deste requisito não será admitida a apresentação de certificação de nível associado, comercias, ou participação em treinamento;

A LICITANTE deverá apresentar comprovação de possuir certificação ISO 27001 comprovando estar apta a prestar o serviço de MONITORAMENTO SOC (Security Operations Center).

25. DO PAGAMENTO

25.1. O pagamento será efetuado pela Contratante no prazo de até 15 (quinze) dias úteis, contados do recebimento da Nota Fiscal/Fatura;

25.2. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência;

25.3. A Nota Fiscal ou Fatura deverá estár obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

25.3.1. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

25.4. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento.

25.5. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

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

25.7. Se, por qualquer motivo alheio à vontade do CONTRATANTE, for paralisada a prestação do serviço, o período correspondente não gerará obrigação de pagamento.

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

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I = (6/100) 365	I = 0,00016438 TX = Percentual da taxa anual = 6%

26. DAS SANÇÕES ADMINISTRATIVAS

26.1. Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar a CONTRATADA as seguintes sanções:

26.1.1. **Advertência** por escrito formal ao fornecedor, em decorrência de atos menos graves e que ocasionem prejuízos para a Administração (CONTRATANTE), desde que não caiba a aplicação de sanção mais grave e, se for o caso, conferindo prazo para a adoção de medidas corretivas cabíveis;

26.1.2. **Multas** na forma abaixo:

a) multa de 2,0% (dois por cento) por dia sobre o valor nota de empenho em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

b) multa de 30% (trinta por cento) sobre o valor da nota de empenho, em caso de inexecução total da obrigação assumida;

c) multa de 10% (dez por cento) aplicado sobre o percentual de 20% (vinte por cento) do valor da proposta do licitante, por ilícitos administrativos no decorrer do certame, tais como:

I - Interposição de recursos manifestamente protelatórios;

II - Deixar de entregar documentação exigida para o certame;

III - Desistência da proposta, salvo por motivo justo decorrente de fato superveniente e aceito pela Administração;

IV - Não cumprimento dos requisitos de habilitação na modalidade pregão, embora o licitante tenha declarado previamente no certame que os cumpria;

V - Não apresentação da nova proposta no prazo estabelecido, na modalidade pregão, consoante valor ofertado nas fases de lances ou de negociação;

VI - Tumultuar a sessão pública da licitação.

VII - Convocada dentro do prazo de validade da sua proposta, não assinar contrato;

VIII - Falhar na execução do contrato;

IX - Fraudar a execução dcontrato;

X - Apresentar comportamento inidôneo;

XI - Cometer fraude fiscal;

XII - Fazer declaração falsa.

XIII - Cadastrar propostas comerciais eletrônicas com valores exorbitantes em relação ao valor máximo;

XIV - Não apresentação de situação fiscal e trabalhista regular no ato da assinatura do contrato;

26.1.3. **Suspensão de licitar** e de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos.

26.1.4. **Impedimento de licitar** e de contratar com Estado do Acre (Tribunal de Justiça do Estado do Acre) e o descredenciamento no SICAF, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta: I - não assinar o contrato ou a ata de registro de preços; II - não entregar a documentação exigida no edital; III - apresentar documentação falsa; IV - causar o atraso na execução do objeto; V - não mantiver a proposta; VI - falhar na execução do contrato; VII - fraudar a execução do contrato; VIII - comportar-se de modo inidôneo; IX - declarar informações falsas; e X - cometer fraude fiscal.

26.1.5. **Declaração de inidoneidade** para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir o **CONTRATANTE** pelos prejuízos causados e depois de decorrido o prazo não superior a 02 (dois) anos previsto no inciso IV do artigo 87 da Lei n. 8.666, de 21 de junho de 1993.

26.2. O **CONTRATANTE** não aplicará a multa de mora quando optar por realizar as reduções no pagamento previsto neste instrumento, sendo vedada a dupla penalização da **CONTRATADA** pelo fato (atraso) na execução dos serviços.

26.3. Pelo descumprimento das obrigações assumidas a Administração aplicará multas conforme a gradação estabelecida nas tabelas seguintes:

TABELA 1

GRAU	CORRESPONDÊNCIA
1	2 % (dois por cento) sobre o valor da nota de empenho.
2	3 % (três por cento) sobre o valor da nota de empenho.
3	15% (quinze por cento) sobre o valor da nota de empenho.
4	30% (trinta por cento) sobre o valor da nota de empenho.

TABELA 2

ITEM	DESCRIÇÃO	GRAU
1	Não apresentação de situação fiscal e trabalhista regular no ato da assinatura do contrato.	4
2	Recusar-se a assinar o contrato dentro do prazo previsto no edital do certame.	4
3	Deixar de substituir os materiais quando recusados pelo ÓRGÃO	3
4	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, a entrega dos materiais adquiridos.	1
5	Não apresentação de situação fiscal e trabalhista regular no ato da assinatura da emissão da nota de empenho	2
6	Não retirar a nota de empenho.	3

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

26.7. O prazo para apresentação de recursos das penalidades aplicadas é de 05 (cinco) dias úteis, contados da data de recebimento da notificação.

26.8. O recurso será dirigido ao Diretor de Logística, que poderá rever sua decisão em 05 (cinco) dias, ou, no mesmo prazo, encaminhá-lo, devidamente informado, à autoridade superior para análise, em igual prazo.

26.9. Da aplicação da penalidade de declaração de inidoneidade, prevista no subitem 11.3.5., caberá pedido de reconsideração, apresentado ao Presidente do TJAC, no prazo de 10 (dez) dias úteis a contar da data da intimação.

26.10. Se houver aplicação de multa, esta será descontada de qualquer fatura ou crédito existente no TJAC em nome da fornecedora e, caso seja a mesma de valor superior ao crédito existente, a diferença a ser cobrada administrativa ou judicialmente.

26.11. As multas não têm caráter indenizatório e seu pagamento não eximirá a CONTRATADA de ser acionada judicialmente pela responsabilidade civil derivada de perdas e danos junto ao CONTRATANTE, decorrentes das infrações cometidas.

26.12. Não será aplicada multa se, comprovadamente, o atraso na entrega dos materiais, advieram de caso fortuito ou motivo de força maior;

26.13. Da sanção aplicada caberá recurso, no prazo de 5 (cinco) dias úteis da notificação, à autoridade superior àquela que aplicou a sanção.

27 GARANTIA DA EXECUÇÃO

27.1. Não haverá exigência de garantia contratual da execução.

28 REAJUSTE

28.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

28.1.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

28.1.1.1. Os valores contratados serão reajustados com base na variação do IPC-fipe, calculado e divulgado pelo Instituto de Pesquisas Econômicas - USP, de acordo com a seguinte fórmula:

$R=(\frac{I-Io}{Io}).p$ onde:

R: = Reajuste

I = Nº índice da data do reajuste

Io = Nº índice da data limite da apresentação da proposta ou da concessão do último reajuste

P = Preço a ser reajustado.

28.2. A aplicação da fórmula supracitada vincula-se à divulgação do índice oficial do mês de reajuste, não devendo ser utilizado o cálculo pró-rata, mas sim o mês cheio.

28.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

29. DAS VEDAÇÕES

29.1. É vedado à CONTRATADA:

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

29.1.2. Transferir a terceiros, ou subcontratar o objeto, exceto serviços acessórios e correlatos ao objeto, tais como instalação e treinamento.

29.1.3. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a CONTRATANTE pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da contratação. Colocar na informação que é uma situação pontual de operadoras.

30. DAS ALTERAÇÕES

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

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

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

31. DA RESCISÃO

31.1. O presente Contrato poderá ser rescindido:

31.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

31.1.2. amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

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

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

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

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

31.4.2. Relação dos pagamentos já efetuados e ainda devidos;

31.4.3. Indenizações e multas.

32. VALOR ESTIMADO DA CONTRATAÇÃO:

32.1. O valor total estimado da contratação é o constante no Mapa de preços,evento nº 0955844.

32.2. Metodologia aplicada à pesquisa de preços:

De acordo com o Art. 2º da Instrução Normativa nº 3, de 20 de abril de 2017, as quais dispõem sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, a pesquisa de preços deve ser realizada:

I - Painel de Preços disponível no endereço eletrônico http://paineldeprecos.planejamento.gov.br;
II - contratações similares de outros entes públicos, em execução ou concluídos nos 180 (cento e oitenta) dias anteriores à data da pesquisa de preços;
III - pesquisa publicada em mídia especializada, sítios eletrônicos especializados ou de domínio amplo, desde que contenha a data e hora de acesso;
IV - pesquisa com os fornecedores, desde que as datas das pesquisas não se diferenciem em mais de 180 (cento e oitenta) dias.
§1º Os parâmetros previstos nos incisos deste artigo poderão ser utilizados de forma combinada ou não, devendo ser priorizados os previstos nos incisos I e II e demonstrado no processo administrativo a metodologia utilizada para obtenção do preço de referência.
§2º Serão utilizados, como metodologia para obtenção do preço de referência para a contratação, a média, a mediana ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros adotados neste artigo, desconsiderados os valores inexequíveis e os excessivamente elevados.
§ 3º Poderão ser utilizados outros critérios ou metodologias,desde que devidamente justificados pela autoridade competente.
§ 4º Os preços coletados devem ser analisados de forma crítica, em especial, quando houver grande variação entre os valoresapresentados.
§ 5º Para desconsideração dos preços inexequíveis ou excessivamenteelevados, deverão ser adotados critérios fundamentadose descritos no processo administrativo.
§ 6º Excepcionalmente, mediante justificativa da autoridade competente, será admitida a pesquisa com menos de três preços ou fornecedores.

33 DAS MEDIDAS ACAUTELADORAS:

33.1. Consoante o artigo 45 da Lei nº 9.784, de 1999, a Administração Pública poderá, sem a prévia manifestação do interessado, motivadamente, adotar providências acauteladoras, inclusive retendo o pagamento, em caso de risco iminente, como forma de prevenir a ocorrência de dano de difícil ou impossível reparação.

34. DOS CASOS OMISSOS:

34.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 10.520, de 17 de julho de 2002, Lei Complementar nº 123/2006, as disposições contidas na Lei nº 8.078,de 1990 – Código de Defesa do Consumidor, Decretos Federais nº 3.555/2000, 10.024/2019, 7.892/2013, 9.488/2018 e o Decreto Estadual nº 4.767/2019, aplicando-se, subsidiariamente, as disposições da Lei n.º 8.666/1993, supletivamente a teoria geral dos contratos, e subordinando-se às condições e exigências estabelecidas neste Edital e seus anexos.

Rio Branco-AC, 21 de julho de 2021.

Documento assinado eletronicamente por **Helio Oliveira de Carvalho**, **Gerente**, em 28/07/2021, às 13:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjac.jus.br/verifica informando o código verificador **1010100** e o código CRC **861D9417**.