CUIABÁ-MT, 01 DE JUNHO DE 2022 - TERMO DE REFERÊNCIA Nº 08.7/2022.

1. DO OBJETO

1.1. Este Termo de Referência tem como objeto a contratação de empresa especializada para fornecimento de Solução Integrada de Link de Internet via fibra óptica de 150 (cento e cinquenta) Mbps com SD-WAN Segura (provimento de serviços de segurança, administração dos serviços providos, gestão de vulnerabilidades da rede de computadores e resposta a incidentes de segurança com transferência de conhecimento) e Solução de rede Wireless (sem fio) via fibra óptica de 150 (cento e cinquenta) Mbps, para atender o Conselho Regional de Contabilidade de Mato Grosso.

1.2. Deverá possuir solução integrada composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) que tenha a capacidade de integrar em um único dispositivo: filtro de pacotes com controle de estado, camada de antivírus, filtro de conteúdo WEB, filtro Antispam, VPN, IDS/IPS, balanceamento de carga, QoS e Proxy reverso, com o objetivo de prover acesso aos sistemas online e garantir disponibilidade e segurança dos sistemas web.

1.3. Esta contratação deverá contemplar todo o licenciamento, suporte técnico, instalação, ativação e configuração dos equipamentos, conforme especificações detalhadas neste Termo de Referência.

2. DA JUSTIFICATIVA DA CONTRATAÇÃO

2.1 Do Link dedicado de internet

2.1.1. Tendo em vista a impossibilidade de se realizar as tarefas diárias sem o acesso internet, a implementação de novos sistemas web, a utilização em sistemas de telefonia Voip, a disponibilidade de serviços web para toda classe contábil, o uso de ferramentas que demandam uma maior quantidade de banda de internet, como transmissões de palestras, cursos, reuniões de forma on-line, e demandas futuras, faz-se necessária a contratação do link de internet, bem como o aumento da velocidade para download e upload. O link é responsável por sustentar toda utilização da Internet dentro do órgão e todos os serviços disponíveis ao público externo.

2.1.2. Esse cenário contempla o fato de que a Internet exerce papel preponderante para que a CRCMT consiga satisfazer, com efetividade, sua missão institucional fornecendo diversos serviços, dentre eles: Serviços On-Line, sistema eletrônico de Registro, sistema eletrônico de Fiscalização, certidões, Emissão de guias, Alvarás, decore, dentre outros.

2.1.3. Os setores de Registro e de Fiscalização do CRCMT vêm, gradativamente, migrando seus processos de trabalho manuais para o meio eletrônico, onde frequentemente novos sistemas são implantados, dependentes da disponibilidade dos serviços de infraestrutura de telecomunicações, fazendo-se necessária a contratação de uma nova rede de telecomunicações de maior capilaridade e menor custo, com recursos de conectividade à Internet e que venham a permitir acesso aos sistemas.

2.1.4. Adicionalmente, houve nos últimos anos um aumento de competitividade no mercado estadual com a entrada de novos fornecedores, promovendo um aumento de oferta de serviços de telecomunicações. Este aumento representa uma oportunidade potencial para o

CRCMT em firmar contratos com melhor relação custo/benefício do que o praticado nos últimos anos.

2.2 Do Gateway SD-WAN Seguro

2.2.1. Garantirá uma maior proteção entre a rede externa (wan) e a rede interna (lan) do CRCMT, protegendo os dados públicos de ataques externos. Outra funcionalidade do software será o gerenciamento das conexões dos usuários da internet possibilitando a interrupção imediata de qualquer acesso suspeito e inapropriado. A solução buscar gerenciar a utilização da internet pelos usuários, definindo regras de utilização, bem como taxa de utilização por usuário e prioridades entre aplicações e protocolos, evitando que alguma aplicação utilize demasiadamente a banda de internet disponibilizada pelo provedor em detrimento dos demais.

2.2.2. A solução permite criar regras para utilização, onde será possível efetuar auditoria sobre os acessos, identificando o autor de alguma transgressão, se necessário. A solução gerenciará a utilização da internet, permitindo o uso mais consciente e menos invasivo da internet.

2.2.3. O advento de novas ameaças tecnológicas requer a adoção de novas soluções de segurança para garantir a integridade dos dados armazenados dentro da nossa infraestrutura de tecnologia da informação.

2.2.4. A solução deverá conter atualização constante para garantir a excelência da tecnologia empregada, visando antecipar-se a possíveis falhas, brechas e problemas de segurança. As quantidades especificadas têm o objetivo de garantir segurança e alta disponibilidade dos serviços de tecnologia da informação do CRCMT.

2.2.5. O CRCMT está dividido em diversos setores, sendo fundamental a integração entre esses setores e o monitoramento da estrutura de informática, sendo peça fundamental o controle centralizado sobre o acesso da internet. Este projeto visa a eficácia das operações de TIC (Tecnologia da Informação e Comunicação) através da unificação, simplificação e ampliação do gerenciamento dos serviços, atingindo redução de custos e otimização da infraestrutura.

2.2.6. O sistema deverá proporcionar consciência situacional sobre as vulnerabilidades e malwares que podem afetar a segurança da informação no Conselho Regional de Contabilidade de Mato Grosso.

2.3. Da Solução de rede Wireless

2.3.1 Atualmente, no que tange a disponibilização de uma rede de acesso à internet sem fio nos ambientes do CRCMT, não se resume apenas na implantação de recursos tecnológicos (modens, roteadores e etc.), mas sim a todo um processo de gerenciamento e controle dos usuários e dos conteúdos acessados por estes utilizadores. A solução a ser adquirida tem como objetivo prover um serviço de internet sem fio de qualidade para os registrados e demais visitantes do órgão, entretanto com toda a segurança e controle sobre os acessos realizados na rede corporativa, considerando a necessária proteção e responsabilidade sobre conteúdo acessado pelos usuários dentro de sua rede; visando impedir a transmissão e recepção de tráfego nocivo, identificar, prevenir e bloquear tentativas de intrusão, realizar serviços de filtro de conteúdo web, monitorar e regular as solicitações feitas a aplicações

web, fazer a gestão das vulnerabilidades encontradas em sistemas e recursos de TI e monitorar eventos que possam afetar a segurança computacional da instituição;

2.3.2. As redes wireless minimizam os custos associados à instalação de cabos e à realização de obras emergenciais, com vantagens claras para a manutenção da infraestrutura e gestão dos recursos de rede, que tornam-se muito mais simples;

2.3.3. Possibilitar o acesso de profissionais , conselheiros , servidores e visitantes à Internet, Intranet e sistemas corporativos, através de uma rede de dados local (LAN – Local Area Network) sem fio, sem a dependência de pontos fixos de rede instalados próximo aos usuários;

2.3.4. Permitir o acesso ao sinal de wifi a todos profissionais e visitantes, partipantes de cursos, congressos, eventos, workshops, palestras, etc...;

2.3.5. Promover maior agilidade na implantação e ampliação LAN para inserção de novos dispositivos;

2.3.6. Facilidade de instalação, portabilidade e escalabilidade;

2.3.7. Implementação rápida e simples em comparação com a ampliação do quantitativo dos pontos fixos existentes, que demanda um projeto de engenharia e a execução de uma obra de infraestrutura de cabeamento estruturado.

2.3.8. A rede atualmente cabeada (metálica) será mantida, permitindo a este Regional dispor de uma rede “física” híbrida (metálica e wireless) e selecionar a melhor solução para a instalação de novos dispositivos de rede;

2.3.9. A rede wireless em questão visa garantir a segurança da rede interna , uma vez que sua conexão será feita a partir de outra rede local especifica, via fibra óptica, com o intuído de minimizar e mitigar riscos a rede local , bem como a segurança interna do CRCMT.

2.3.10. A solução permite criar regras para utilização, onde será possível efetuar auditoria sobre os acessos, identificando o autor de alguma transgressão, se necessário. A solução gerenciará a utilização da internet, permitindo o uso mais consciente e menos invasivo da internet.

2.3.11 Uso de soluções de tecnologia da informação integradas e seguras, adequando a aplicação dos recursos às estratégias institucionais, para modernizando da plataforma tecnológica e infraestrutura, mediante a adoção de padrões tecnológicos e soluções que alcancem a efetividade dos objetivos já expostos, conferindo produtividade, eficiência e eficácia na prestação de serviços com segurança, disponibilidade, desempenho; satisfação dos usuários;

2.3.12. O advento de novas ameaças tecnológicas requer a adoção de novas soluções de segurança para garantir a integridade dos dados armazenados dentro da nossa infraestrutura de tecnologia da informação.

3. DA FUNDAMENTAÇÃO LEGAL

3.1. A contratação do serviço seguirá os amparos legais da Lei nº 14.133/21, levando em consideração o Art. 75, inciso II:

“Art. 75. É dispensável a licitação:

(...)

II – para contratação que envolva valores inferiores a R$ 50.000,00 (cinquenta mil reais) o caso de outros serviços e compras;

4. BENEFÍCIOS ESPERADOS COM A CONTRATAÇÃO

4.1 Do Link dedicado de internet

4.1.1. O objetivo com a nova contratação é melhorar a qualidade dos serviços prestados possibilitando acesso à Internet de forma descentralizada e a comunicação direta entre os diversos pontos de presença com menor custo possível.

4.1.2. Com o aumento deste link e mais o balanceamento de carga, projeta-se que a situação permita a qualidade e estabilização dos serviços, bem como atenda demandas futuras.

4.1.3. O CRCMT trabalha com vários serviços via web, os setores de Registro e Fiscalização migraram seus processos de trabalho manuais para o meio eletrônico. Portanto para funcionamento destes sistemas, necessita-se de internet intermitente e com capacidade alta de acesso. Uma internet ruim acarretará na deficiência do atendimento dos profissionais e empresas ligadas ao CRCMT, ocasionando transtornos ou mesmo prejuízos aos mesmos por deficiência de acesso.

4.1.4. Desta forma os sistemas poderão ser disponibilizados no sítio obedecendo aos planos de continuidade pré-estabelecidos, garantindo disponibilidade, integridade e confiabilidade.

4.2 Do Gateway SD-WAN Seguro

4.2.1. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

4.2.2. Maior visibilidade do tráfego de rede e aplicações, possibilitando a detecção e proteção em tempo real contra ameaças;

4.2.3. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

4.2.4. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.

4.2.5. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.

4.2.6. Criação de políticas de proteção da rede contra eventuais ataques de usuários mal intencionados através do fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;

4.2.7. Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);

4.2.8. Melhor filtro de conteúdo URL, sancionando acesso a sites indesejados de conteúdo ilícito.

4.3. Da Solução de rede Wireless

4.3.1. As redes wireless minimizam os custos associados à instalação de cabos e à realização de obras emergenciais, com vantagens claras para a manutenção da infraestrutura e gestão dos recursos de rede, que tornam-se muito mais simples;
4.3.2. A solução deverá conter atualização constante para garantir a excelência da tecnologia empregada, visando antecipar-se a possíveis falhas, brechas e problemas de segurança. As quantidades especificadas têm o objetivo de garantir segurança e alta disponibilidade dos serviços de tecnologia da informação do CRCMT.

4.3.3. Este projeto visa a eficácia das operações de TIC (Tecnologia da Informação e Comunicação) através da unificação, simplificação e ampliação do gerenciamento dos serviços, atingindo redução de custos e otimização da infraestrutura.

4.3.4. Adequação às legislações vigentes, tais como Marco Civil da Internet Lei nº 12.965/2014 e todas as exigências da LGPD (Lei Geral de Proteção de Dados);

4.3.5. Guarda os registros de acesso por 6 meses, como determina a Lei 12.965/ 14;

5. DA ESPECIFICAÇÃO DO OBJETO

5.1. Solução Integrada de Link de Internet com SD-WAN Segura na modalidade locação para o Conselho Regional de Contabilidade se dará conforme tabela abaixo:

Produto 1	Localidade	Qtde
Link de Internet de 150 MBPS com SD-WAN Segura.	Sede CRC/MT	1
Gerência Centralizada.	Sede CRC/MT	1
Serviço de Instalação da Solução.	Sede CRC/MT	1
Suporte e Garantia Técnica da Solução.	Sede CRC/MT	1
Produto 2	Localidade	Qtde
Solução de rede Wireless (sem fio) via fibra óptica de 150 (cento e cinquenta) Mbps.	Sede CRC/MT	1
Gerência Centralizada.	Sede CRC/MT	1
Serviço de Instalação da Solução.	Sede CRC/MT	1
Suporte e Garantia Técnica da Solução.	Sede CRC/MT	1

5.2. A Licitante deverá realizar a instalação dos produtos de segurança contratados;

5.3. O fornecedor deverá entregar o Link de dados para acesso à internet dedicada com solução integrada de segurança instalado e configurado e o Link da solução para acesso à internet de acordo com os padrões fornecidos pela equipe técnica da contratante.

5.4. Internet suportada por serviço de comunicação de dados de alta capacidade, incluindo gerenciamento e controle de acesso Wi-Fi, internet segura, rápida;

5.5. Internet e gerenciamento em um único produto;

5.6. Opção de acesso com login Social (Facebook, Google, E-mail, SMS);

5.7. Guarda dos registros de acesso por 6 meses, como determina a Lei 12.965/ 14;

5.8. Suporte remoto;

5.9. Bloqueio de usuários;

5.10 Veicula promoção facebook;

5.11. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

5.12. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais;

5.13. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.

5.14. Melhor filtro de conteúdo URL, sancionando acesso a sites indesejados de conteúdo ilícito.

5.15. Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
5.16. Deve suportar o acesso via web (https) para gerenciamento da solução;

5.17. Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) no console de gerenciamento;

5.18. Cada hardware deverá ser fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoração, cabendo inclusive, a CONTRATADA, a instalação do hardware e configurações de todas as funcionalidades da solução;

5.19. Toda a solução deve ser nova, disponível para primeiro uso e em pleno período de vida, sem previsão de término dos tempos de vida, vendas e suporte;

6. DOS REQUISITOS DA CONTRATAÇÃO

6.1. LINK DE INTERNET COM SD-WAN SEGURA.

6.1.1. A velocidade do Link contratado deverá ser de no mínimo 100% nos dois sentidos, download e upload;

6.1.2. Disponibilidade 24 (vinte e quatro) horas por dia, durante 07 (sete) dias da semana, a partir de sua ativação até o término do contrato;

6.1.3. O serviço de Internet a ser fornecido, deverá trafegar em um único link, evitando-se deste modo, a instalação de vários links com taxas de transferências inferiores ao solicitado;

6.1.4. Garantia total da banda contratada com redundância;

6.1.5. Ser provido com base em uma infraestrutura de fibra-óptica, como meio de acesso, vedada a utilização de qualquer outra tecnologia de acesso;

6.1.6. A rede de energia elétrica, o sistema de aterramento, condicionamento de ar e segurança física será de responsabilidade do Conselho Regional de Contabilidade;

6.1.7. A Contratada deverá implementar o aumento da velocidade, quando solicitado, sem interrupção do serviço, onde as atualizações tecnológicas requisitadas para este aumento, devem ser suportadas pelos recursos e equipamentos envolvidos na solução desde a instalação inicial;

6.1.8. Todos os equipamentos e enlaces fornecidos pela contratada, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área – ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (International Telecommunication Union), ISO (International Standardization Organization), IEEE (Institute of Electrical and Electronics Engineers), EIA/TIA (Electronics Industry Alliance and Telecomumnication Industry Association);

6.1.9. Prestar serviço de gerenciamento incluindo a disponibilização de uma "Central de Atendimento" e de um Sistema de Monitoramento do Tráfego Internet, via WEB, para acompanhamento dos serviços prestados pelas contratadas;

6.1.10. A Central de Atendimento deverá estar disponível para o contato dos técnicos do Conselho Regional de Contabilidade e se dará através de ligações telefônicas gratuitas, tipo 0800;

6.1.11. Os funcionários de atendimento da contratada devem conhecer todos os serviços contratados e relacionado com a solução, objeto deste instrumento;

6.1.12. Caso haja a necessidade de realizar manutenção preventiva da solução, a contratada deverá formalizar via e-mail o Conselho Regional de Contabilidade, com no mínimo 06 (seis) dias úteis de antecedência da data proposta para a realização do serviço;

6.1.13. A contratada deverá realizar atividades de suporte à conectividade relacionado com a solução em um regime de 24 (vinte quatro) horas por dia, 07 dias na semana;

6.1.14. Os recursos de hardware e software dos equipamentos envolvidos devem ser atualizados tecnologicamente, sem ônus para a Contratante, durante a vigência do contrato;

6.1.15. Sempre que houver lançamento de nova versão de sistema operacional e ou firmware que faça correções de segurança dos serviços prestados, as contratadas deverão providenciar as devidas atualizações com prévia aprovação do Conselho Regional de Contabilidade, sem ônus para a Contratante.

6.1.16. Os equipamentos relacionados com a solução deverão ser instalados e mantidos operacionais, com todos os seus acessórios e documentações.

6.1.17. A Contratada deverá vir até a sala de telecomunicações da Coordenadoria de Informática e fazer um estudo para melhor forma de acomodar os equipamentos com o objetivo de aperfeiçoar o espaço.

6.1.18. A latência média máxima permitida será de 50ms, considerando o tempo calculado entre o instante de transmissão de um pacote e o recebimento do mesmo em seu destino e serão calculados pelo tempo de resposta médio de 10 "pings" de 32 bytes transmitidos a cada 5 minutos do roteador instalado na DTI para o backbone da Contratada, contabilizadas mensalmente.

6.2. Da solução de rede Wireless

6.2.1. A velocidade do Link contratado deverá ser de no mínimo 100% nos dois sentidos, download e upload;

6.2.2. Disponibilidade 24 (vinte e quatro) horas por dia, durante 07 (sete) dias da semana, a partir de sua ativação até o término do contrato;

6.2.3. O serviço de Internet a ser fornecido, deverá trafegar em um único link, evitando-se deste modo, a instalação de vários links com taxas de transferências inferiores ao solicitado;

6.2.4. Garantia total da banda contratada com redundância;

6.2.5. Ser provido com base em uma infraestrutura de fibra-óptica, como meio de acesso, vedada a utilização de qualquer outra tecnologia de acesso;

6.2.6. A rede de energia elétrica, o sistema de aterramento, condicionamento de ar e segurança física será de responsabilidade do Conselho Regional de Contabilidade;

6.2.7. A Contratada deverá implementar o aumento da velocidade, quando solicitado, sem interrupção do serviço, onde as atualizações tecnológicas requisitadas para este aumento, devem ser suportadas pelos recursos e equipamentos envolvidos na solução desde a instalação inicial;

6.2.8. Todos os equipamentos e enlaces fornecidos pela contratada, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área – ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (International Telecommunication Union), ISO (International Standardization Organization), IEEE (Institute of Electrical and Electronics Engineers), EIA/TIA (Electronics Industry Alliance and Telecomumnication Industry Association);

6.2.9. Prestar serviço de gerenciamento incluindo a disponibilização de uma “Central de Atendimento” e de um Sistema de Monitoramento do Tráfego Internet, via WEB, para acompanhamento dos serviços prestados pelas contratadas;

6.2.10. A Central de Atendimento deverá estar disponível para o contato dos técnicos do Conselho Regional de Contabilidade e se dará através de ligações telefônicas gratuitas, tipo 0800;

6.2.11. Os funcionários de atendimento da contratada devem conhecer todos os serviços contratados e relacionado com a solução, objeto deste instrumento;

6.2.12. Caso haja a necessidade de realizar manutenção preventiva da solução, a contratada deverá formalizar via e-mail o Conselho Regional de Contabilidade, com no mínimo 06 (seis) dias úteis de antecedência da data proposta para a realização do serviço;

6.2.13. A contratada deverá realizar atividades de suporte à conectividade relacionado com a solução em um regime de 24 (vinte quatro) horas por dia, 07 dias na semana;

6.2.14. Os recursos de hardware e software dos equipamentos envolvidos devem ser atualizados tecnologicamente, sem ônus para a Contratante, durante a vigência do contrato;

6.2.15. Sempre que houver lançamento de nova versão de sistema operacional e ou firmware que faça correções de segurança dos serviços prestados, as contratadas deverão providenciar as devidas atualizações com prévia aprovação do Conselho Regional de Contabilidade, sem ônus para a Contratante.

6.2.16. Os equipamentos relacionados com a solução deverão ser instalados e mantidos operacionais, com todos os seus acessórios e documentações.

6.2.17. A Contratada deverá vir até a sala de telecomunicações da Coordenadoria de Informática e fazer um estudo para melhor forma de acomodar os equipamentos com o objetivo de aperfeiçoar o espaço.

6.2.18. A latência média máxima permitida será de 50ms, considerando o tempo calculado entre o instante de transmissão de um pacote e o recebimento do mesmo em seu destino e serão calculados pelo tempo de resposta médio de 10 “pings” de 32 bytes transmitidos a cada 5 minutos do roteador instalado na DTI para o backbone da Contratada, contabilizadas mensalmente.

6.3. GARANTIA E ATUALIZAÇÃO DE SOFTWARE.

6.3.1. Atualização do software embarcado durante o período de 12 meses;

6.3.2. Atualização do sistema operacional embarcado durante o período de 12 meses;

6.3.3. No preço deverá estar incluído todo o software necessário para atender as características exigidas, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

7. DA ESPECIFICAÇÃO TÉCNICA DO OBETO

7.1. GERAL.

7.1.1. A CONTRATADA deverá informar na proposta, o fabricante e os modelos dos hardwares que serão utilizados;

7.1.2. Cada hardware deverá ser fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoração, cabendo inclusive, a CONTRATADA, a instalação do hardware e configurações de todas as funcionalidades da solução;

7.1.3. Toda a solução deve ser nova, disponível para primeiro uso e em pleno período de vida, sem previsão de término dos tempos de vida, vendas e suporte;

7.1.4. A solução de SD-WAN deverá ser entregue em hardware dedicado;

7.1.5. Caso a solução de SD-WAN seja baseada em software, deverá ser fornecido o respectivo hardware.

7.2. DO GATEWAY SD-WAN SEGURO – TIPO 1.

7.2.1. Físicas:

7.2.1.1. Deve possuir no mínimo interface de console serial via RJ45 ou USB;

7.2.1.2. Deve possuir no mínimo 5 (cinco) interfaces RJ45-UTP, podem ser fornecidas interfaces SFP desde que com transceiver RJ45;

7.2.1.3. Caso o datasheet ou folder do fabricante NGFW da solução ofertada possua métrica relacionado a Ambiente de Produção ou Empresarial, este deve ser considerado como métrica de dimensionamento a atender.

7.2.1.4. Não será aceito métrica de laboratório ou RFC caso a documentação oficial do fabricante possua métricas de Ambiente de Produção ou Empresarial;

7.2.1.5. Throughput de Firewall de no mínimo 5 (cinco) Gigabits e 800 (oitocentos) Mbps;

7.2.1.6. Throughput de Prevenção de Ameaças (funcionalidades ativas de: Firewall, Controle de Aplicação, IPS, Proteção contra Malware) de no mínimo 580 (quinhentos e oitenta) Mbps;

7.2.1.7. Throughput de VPN IPSec de pelo menos 4 (quatro) Gbps e 200 (duzentos) Mbps;

7.2.1.8. Permitir o número de túneis IPSEC Site-to-Site mínimo de 180 (cento e oitenta);

7.2.1.9. Permitir o número de túneis IPSEC Client-to-Site mínimo de 200 (duzentos);

7.2.1.10. Permitir o número de túneis /usuários VPN SSL mínimo de 200 (duzentos);

7.2.1.11. Throughput de inspeção SSL de no mínimo 300 (trezentos) Mbps;

7.2.1.12. Permitir até 700 (setecentos) mil Sessões TCP Concorrentes;

7.2.1.13. Permitir até 33 (trinta e três) mil novas conexões TCP por segundo;

7.2.1.14. Permitir utilizar até 10 (dez) firewalls virtuais;

7.3. GERAL DO GATEWAY SD-WAN SEGURO.

7.3.1. Deve possuir funcionalidades de: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

7.3.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

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

7.3.4. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;

7.3.5. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

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

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

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

7.3.9. Os dispositivos de proteção de rede devem suportar sFlow;

7.3.10. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

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

7.3.12. Deve suportar NAT dinâmico (Many-to-1);

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

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

7.3.15. Deve suportar NAT estático (Many-to-Many);

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

7.3.17. Deve suportar Tradução de porta (PAT);

7.3.18. Deve suportar NAT de Origem;

7.3.19. Deve suportar NAT de Destino;

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

7.3.21. Deve poder combinar NAT de origem e NAT de destino na mesma política;

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

7.3.23. Deve suportar NAT64 e NAT46;

7.3.24. Deve implementar o protocolo ECMP;

7.3.25. Deve suportar SD-WAN de forma nativa;

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

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

7.3.28. 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.

7.3.29. Deve suportar o balanceamento de, no mínimo, três links;

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

7.3.31. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

7.3.32. Enviar log para sistemas de monitoração externos, simultaneamente;

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

7.3.34. Proteção anti-spoofing;

7.3.35. Implementar otimização do tráfego entre dois equipamentos;

7.3.36. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

7.3.37. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

7.3.38. Suportar OSPF graceful restart;

7.3.39. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

7.3.40. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

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

7.3.42. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

7.3.43. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

7.3.44. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

7.3.45. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

7.3.46. A configuração em alta disponibilidade deve sincronizar: Sessões;

7.3.47. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

7.3.48. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

7.3.49. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;

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

7.3.51. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance; Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

7.3.52. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

7.3.53. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

7.3.54. Deve ser fornecida funcionalidade de Inspeção SSL sem limitação de licenciamento caso a solução ofertada possua licenciamento, deve ser fornecido em sua capacidade máxima.

7.3.55. Permitir a integração com repositório de logs de forma segura e otimizada;

7.3.56. Permitir identificar potenciais vulnerabilidades ou ameaças e orquestrar ação de prevenção.

7.3.57. Deve existir um Serviço de Suporte que ofereça apoio do fabricante e atualização de sistema operacional;

7.3.58. O console de administração deve suportar no mínimo inglês, espanhol e português.

7.3.59. O console deve suportar a administração de switches e pontos de acesso para melhorar o nível de segurança;

7.3.60. A solução deve suportar integração nativa de equipamentos de proteção de correio eletrônico, firewall de aplicações, proxy, cache e ameaças avançadas

7.3.61. Deverá suportar controles por zona de segurança;

7.3.62. Controles de políticas por porta e protocolo;

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

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

7.3.65. Deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

7.3.66. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente as políticas de firewall;

7.3.67. Deve suportar automação de situações como detecção de equipamentos comprometidos, estado do sistema, mudanças de configuração, eventos específicos, e aplicar uma ação que possa ser notificação, bloqueio do equipamento, execução de scripts ou funções em nuvem pública.

7.3.68. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);

7.3.69. Deve suportar integração de nuvens públicas e integração SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage e Kubernetes;

7.3.70. Deve suportar integração com Solução de SIEM multi fabricante;

7.3.71. Deve suportar o protocolo padrão da indústria VXLAN;

7.3.72. A solução deve suportar a integração nativa com soluções de sandboxing;

7.3.73. O appliance deve estar licenciado e permitir a utilização de no mínimo 10 (dez) instâncias virtuais;

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

7.3.75. Reconhecer pelo menos 3000 aplicações diferentes, em camada 7, 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 e-mail;

7.3.76. 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;

7.3.77. 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;

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

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

7.3.80. Atualizar a base de assinaturas de aplicações automaticamente;

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

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

7.3.83. 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;

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

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

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

7.3.87. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Hangouts chat e bloquear a chamada de vídeo;

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

7.3.89. 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);

7.3.90. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

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

7.3.92. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;

7.3.93. 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;

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

7.3.95. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

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

7.3.97. 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;

7.3.98. Deve permitir o bloqueio de vulnerabilidades;

7.3.99. Deve incluir proteção contra ataques de negação de serviços;

7.3.100. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;

7.3.101. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;

7.3.102. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;

7.3.103. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;

7.3.104. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes mal formados;

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

7.3.106. Detectar e bloquear a origem de portscans;

7.3.107. Bloquear ataques efetuados por worms conhecidos;

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

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

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

7.3.111. Identificar e bloquear comunicação com botnets;

7.3.112. 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;

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

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

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

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

7.3.117. 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 usuários, origem, destino e zonas de segurança;

7.3.118. Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes incluindo NGFW (Next Generatil Firewall), Sandbox (on-premise ou nuvem);

7.3.119. Deve ser considerado para esta especificação proteção via Sandbox do fabricante do NGFW ou terceiros, na modalidade "in cloud" ou "on premisses", permitindo também na oferta de soluções on premisses, appliances físicos ou virtuais.

7.3.120. Caso seja fornecida solução “on premisses" e em appliance virtual, o servidor de hospedagem e hypervisor também devem ser inclusos nesta oferta.

7.3.121. 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);

7.3.122. 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, em modo de proxy transparente e explícito;

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

7.3.124. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

7.3.125. Possuir pelo menos 60 categorias de URLs;

7.3.126. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

7.3.127. Permitir a customização de página de bloqueio;

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

7.3.129. Além do Explicit Web Proxy, suportar proxy Web transparente;

7.3.130. 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;

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

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

7.3.133. grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

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

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

7.3.136. 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);

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

7.3.138. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

7.3.139. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

7.3.140. Com a finalidade de controlar aplicações de camada 7 e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esses tipos de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

7.3.141. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

7.3.142. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

7.3.143. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

7.3.144. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

7.3.145. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

7.3.146. O QoS deve possibilitar a definição de tráfego com banda garantida;

7.3.147. O QoS deve possibilitar a definição de tráfego com banda máxima;

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

7.3.149. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

7.3.150. Suportar modificação de valores DSCP para o Diffserv;

7.3.151. Suportar priorização de tráfego usando informação de Type of Service;

7.3.152. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

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

7.3.154. Os arquivos devem ser identificados por extensão e tipo;

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

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

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

7.3.158. 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;

7.3.159. Deve contemplar a oferta do licenciamento de DLP caso a solução ofertada possua;

7.3.160. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

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

7.3.162. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

7.3.163. Permitir a utilização das funcionalidades de VPN Site-to-Site e Cliente-To-Site;

7.3.164. Permitir utilizar IPSec VPN sem limitação de licenciamento caso a solução ofertada possua;

7.3.165. Permitir utilizar SSL VPN sem limitação de licenciamento caso a solução ofertada possua;

7.3.166. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

7.3.167. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

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

7.3.169. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

7.3.170. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

7.3.171. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

7.3.172. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

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

7.3.174. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

7.3.175. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

7.3.176. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

7.3.177. Deverá manter uma conexão segura com o portal durante a sessão;

7.3.178. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

7.3.179. SD-WAN:

7.3.179.1. Deverá ser composta por dispositivos SD-WAN (SD-WAN Appliances) e Console de Gerência Centralizada;

7.3.179.2. Os dispositivos SD-WAN (SD-WAN Appliances) podem ser fornecidos em formato de equipamento físico dedicado ou appliance virtual compatível com processadores x86 (ou x64);

7.3.179.3. Em caso de oferta de appliance virtual, a solução deverá ser acompanhada do hardware x86(ou x64) com os pré-requisitos necessários para atender as especificações de performance e interfaces de conectividade descritas neste caderno;

7.3.179.4. Em caso de oferta de appliance virtual, a solução deverá ser acompanhada de um supervisor compatível com os requisitos deste caderno;

7.3.179.5. O SD-WAN deverá suportar vários links de acesso, como MPLS, Internet dedicada e Internet Móvel;

7.3.179.6. Deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

7.3.179.7. Deve possuir capacidade de agregar e balancear, no mínimo, 2 circuitos de dados utilizando uma interface dedicada para cada circuito;

7.3.179.8. Deve permitir a configuração de ISP (rota default estática) com a utilização de probe ou de forma similar para verificar a disponibilidade do provedor. A probe ou similar deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência)

7.3.179.9. Deve balancear o tráfego das aplicações entre múltiplos links simultaneamente;

7.3.179.10. Deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas.

7.3.179.11. Deverá simplificar a implantação de túneis criptografados de site para site;

7.3.179.12. Deverá implementar a PKI usando a autoridade de certificação (CA);

7.3.179.13. Deverá permitir a comunicação indireta entre localidades por meio de topologia "hub and spoke";

7.3.179.14. Deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

7.3.179.15. Deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo;

7.3.179.16. Deverá monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente;

7.3.179.17. A Solução SD-WAN deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados pelos Gateways, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;

7.3.179.18. Deverá suportar arquitetura VRF, onde o tráfego poderá ser segmentado com base em uma definição comum de VRFs em todos os sites;

7.3.179.19. Deverá possuir serviço de servidor DHCP;

7.3.179.20. Deverá possuir serviço de DHCP relay;

7.3.179.21. Deverá implementar rotas estáticas;

7.3.179.22. Deverá implementar OSPF;

7.3.179.23. Deverá implementar BGP;

7.3.179.24. Deve ser possível implementar SD-WAN em alta disponibilidade (pelo menos 2 appliances) no CRCMT e Site Redundante;

7.3.179.25. Deve ser possível implementar SD-WAN utilizando VRRP e realizar a recuperação de falhas através de um roteador compatível com esse protocolo;

7.3.179.26. Deverá suportar aplicativos hospedados em Data Center próprio e também aqueles consumidos como serviço na nuvem;

7.3.179.27. A solução deverá garantir performance de aplicações que utilizam VPN nos sites remotos e serviços de nuvem (SaaS);

7.3.179.28. A solução deverá medir e reagir independentemente à condição de rede UNIDIRECIONALMENTE para todas as condições (Latência, Jitter, Perda, Largura de banda - BW);

7.3.179.29. Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando um dos links está prejudicado;

7.3.179.30. Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando os dois links estão prejudicados;

7.3.179.31. A Solução deverá possuir algum mecanismo de QoS para proteger o tráfego de Internet quanto tiver congestionamento na unidade regional;

7.3.179.32. A Solução deverá permitir que sites de unidades regionais acessem sites VPN legados (não-SD-WAN) sem fazer backhauling do tráfego de aplicativos por meio de um hub SD-WAN;

7.3.179.33. Deve ser possível criar políticas para a modelagem do tráfego definindo pelo menos os parâmetros:

7.3.179.34. IP de Origem;

7.3.179.35. IP de Destino;

7.3.179.36. Porta TCP/UDP de Destino;

7.3.179.37. Domínio e URL de destino;

7.3.179.38. Aplicação de camada 7 utilizada (Office 365, Exchange, SAS, Dropbox, Box, Zoom e etc);

7.3.179.39. Agendamento e gerenciamento de filas;

7.3.179.40. Remarcação de DSCP;

7.3.179.41. Definição dos links utilizados em situação normal;

7.3.179.42. Definição dos links utilizados em caso de falha do(s) link(s) primários;

7.3.179.43. Traffic Shapping;

7.3.179.44. A solução deverá suportar convergência rápida de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas;

7.3.179.45. Poderá ser configurado utilizando perfis e políticas de segurança atribuídos de forma dinâmica;

7.3.179.46. Deverá possuir serviço de Firewall Stateful;

7.3.179.47. Deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

7.3.179.48. A solução deve permitir a inserção automática de serviços de segurança de nuvem, ou seja, com intercepção de tráfego por aplicação e envio a diferentes fornecedores de serviços de segurança em nuvem.

7.3.179.49. A solução deve suportar VPNs do tipo Hub Spoke e Full Mesh;

7.3.179.50. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC de forma segura e criptografada;

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

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

7.3.179.53. Deverá suportar SNMP versões 2c e 3;

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

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

7.3.179.56. A Gerência SD-WAN deverá enviar mensagens syslog referentes aos Gateways SD-WAN para um servidor syslog externo da contratada e da contratante;

7.3.179.57. Deverá realizar medições de latência, Jitter e descarte de pacotes para cada destino em cada uma das interfaces dos Gateways SD-WAN a cada 5 (cinco) minutos no mínimo;

7.3.179.58. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada Gateway SDWAN a cada 5 (cinco) minutos no mínimo;

7.3.179.59. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na GUI da gerência SD-WAN;

7.3.179.60. Possuir os contadores de estatísticas de LAN e WAN dos Gateway SD WAN (bits RX/TX, entrada/saída de pacotes, descartes de pacotes e erros);

7.3.179.61. Deverá ter a capacidade para medir os fluxos de aplicativos como volume de dados trafegados, quantidade de transações entre outros;

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

7.3.179.63. Deverá suportar exportação de registros Netflow / IPFIX/ Netstream baseada em padrões;

7.3.179.64. Deverá possuir provisionamento do Zero Touch que deverá funcionar de tal forma que um CPE SD-WAN seja enviado diretamente do fornecedor de SD-WAN para uma instalação do cliente sem a necessidade de configuração prévia do CPE SD-WAN;

7.3.179.65. Deverá ter a flexibilidade para ser gerenciada pelo cliente e/ou gerenciada pelo parceiro;

7.4. DA GERÊNCIA CENTRALIZADA.

7.4.1. Da Base de Dados Analíticos e Logs:

7.4.1.1. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

7.4.1.2. Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento;

7.4.1.3. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

7.4.1.4. Possuir suporte para SNMP versão 2 e 3;

7.4.1.5. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

7.4.1.6. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

7.4.1.7. Deve estar licenciado, permitindo o uso integrado e operacional de todas as instâncias virtuais NGFW requisitadas;

7.4.1.8. Deve permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS e SSH;

7.4.1.9. Permitir a autenticação de usuários de acesso à plataforma via LDAP;

7.4.1.10. Permitir a autenticação de usuários de acesso à plataforma via Radius;

7.4.1.11. Permitir a autenticação de usuários de acesso à plataforma via TACACS +;

7.4.1.12. Permitir a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

7.4.1.13. Permitir a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

7.4.1.14. Permitir a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

7.4.1.15. Permitir 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;

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

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

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

7.4.1.19. Permitir importação e exportação de relatórios;

7.4.1.20. Deve ter a capacidade de criar relatórios no formato HTML;

7.4.1.21. Deve ter a capacidade de criar relatórios em formato PDF;

7.4.1.22. Deve ter a capacidade de criar relatórios no formato XML;

7.4.1.23. Deve ter a capacidade de criar relatórios no formato CSV;

7.4.1.24. Deve permitir exportar os logs no formato CSV;

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

7.4.1.26. 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;

7.4.1.27. A solução deve ter relatórios predefinidos;

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

7.4.1.29. A duplicação de relatórios existentes deve ser possível para edição posterior;

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

7.4.1.31. 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;

7.4.1.32. 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;

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

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

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

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

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

7.4.1.38. Permitir o envio de relatórios por e-mail automaticamente;

7.4.1.39. Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;

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

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

7.4.1.42. Deve permitir o uso de filtros nos relatórios;

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

7.4.1.44. Permitir especificar o idioma dos relatórios criados;

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

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

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

7.4.1.48. 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;

7.4.1.49. Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, com o objetivo de detectar e corrigir problemas na geração deles;

7.4.1.50. A solução deve permitir importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;

7.4.1.51. Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log;

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

7.4.1.53. Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma;

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

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

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

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

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

7.4.1.59. Deve permitir a criação de incidentes a partir de alertas de eventos para o terminal;

7.4.1.60. Deve permitir a integração ao sistema de tickets do ServiceNow;

7.4.1.61. Deve suportar o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas;

7.4.1.62. Deve suportar o padrão SAML para autenticação do usuário administrador;

7.4.1.63. Deve ter um relatório de uso do aplicativo SaaS;

7.4.1.64. Deve ter um relatório de prevenção de perda de dados (DLP);

7.4.1.65. Deve ter um relatório de VPN;

7.4.1.66. Deve ter um relatório IPS (Intruder Prevention System);

7.4.1.67. Deve ter um relatório de reputação do cliente;

7.4.1.68. Deve ter um relatório de análise de segurança do usuário;

7.4.1.69. Deve ter um relatório de análise de ameaças cibernéticas;

7.4.1.70. Deve ter um relatório diário resumido de eventos e incidentes de segurança;

7.4.1.71. Deve ter um relatório de tráfego DNS;

7.4.1.72. Deve ter um relatório de tráfego de e-mail;

7.4.1.73. Deve ter um relatório dos 10 principais aplicativos usados na rede;

7.4.1.74. Deve ter um relatório dos 10 principais sites usados na rede;

7.4.1.75. Deve ter um relatório de uso de mídia social;

7.5. GARANTIA E ATUALIZAÇÃO DE SOFTWARE.

7.5.1. Atualização do software embarcado durante o período de 12 meses;

7.5.2. Atualização do sistema operacional embarcado durante o período de 12 meses;

7.5.3. No preço deverá estar incluído todo o software necessário para atender as características exigidas, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

8. DO SUPORTE TÉCNICO

8.1. A contratada deverá encaminhar ao CRCMT, em prazo máximo de 10 (dez) dias úteis ao da assinatura do contrato, documento informando todos os procedimentos e números de contato necessários para abertura de chamados de suporte técnico.

8.2. Os chamados de suporte devem ser feitos através de e-mail ou número telefônico 0800, fornecendo neste momento o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos.

8.3. O tempo de solução ou tempo para reparo, que compreende o tempo entre a abertura do chamado técnico até a sua efetiva solução, será no máximo de 6 (seis) horas.

9. DA GARANTIA DOS EQUIPAMENTOS

9.1. Os equipamentos deverão ter garantia durante todo período contratado;

9.1.2. Durante todo o período de garantia a contratada será responsável juntamente com o fabricante pelo atendimento aos chamados para assistência técnica corretiva e substituição de equipamentos defeituosos;

9.1.3. Em caso de inoperância dos equipamentos ou da solução, a CONTRATADA deverá atender a solicitação de correção no prazo máximo de até 4(quatro) horas a partir da abertura da chamada;

9.1.4. Se por ventura, houver a necessidade de substituição dos equipamentos ou da solução, a CONTRATADA deverá atender em até 1(um) dia, sem ônus para o CRCMT.

10. DA EXECUÇÃO E DO PRAZO DE PRESTAÇÃO DOS SERVIÇOS

10.1. A licitante vencedora deverá iniciar a prestação dos serviços objeto deste Termo de Referência, imediatamente após a assinatura do contrato e do fornecimento de ordem de serviço.

10.2. Todos os serviços a serem prestados, terão a fiscalização e participação de empregados do setor de T.I.;

10.3. Deverão ser preparados e apresentados relatórios sobre o planejamento e execução das atividades;

10.4. Deverá ser estabelecido um único responsável pelos serviços que será o ponto de contato entre a contratada e a contratante;

10.5. A Contratada deverá fornecer todas as ferramentas, materiais, equipamentos e acessórios necessários, respeitando-se as normas vigentes e sem qualquer ônus à Contratante;

10.6. É de responsabilidade da contratada, todo o fornecimento e instalação de tubulações, obras civis, acessórios e suporte para o atendimento do serviço. O lançamento de cabo interno será por conta da contratada;

10.7. O CRCMT se reserva o direito de avaliar as características técnicas especificadas por seus próprios meios ou por intermédio de terceiros por ele designados;

10.8. Todo acesso às instalações do CRCMT por pessoal técnico da contratada ou de seus prepostos, deverá ser previamente comunicado ao Coordenador da T.I, telefone (65) 99987-2614;

10.9. Para emissão da ordem de fornecimento pelo CRCMT de todos os circuitos e serviços, as seguintes condições devem ser satisfeitas, concomitantemente:

10.9.1. Estabelecimento de uma conexão entre os roteadores em ambas as pontas;

10.9.2. Acesso a sites na internet;

10.9.3. Disponibilidade de no mínimo 99,9% (noventa e nove, nove por cento) de banda contratada.

11. DAS OBRIGAÇÕES DAS PARTES

Obriga-se a CONTRATADA a:

11.1. Iniciar a prestação dos serviços de acordo com o prazo informado na proposta;

11.2. Responder pelos danos causados diretamente ao CRCMT ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CRCMT;

11.3. Arcar com despesas decorrentes de qualquer infração, seja qual for, desde que praticada por seus técnicos durante a execução dos serviços, ainda que no recinto do CRCMT;

11.4. Arcar com todos os ônus necessários à completa execução dos serviços, inclusive com a implantação e configuração dos softwares e hardwares, se for o caso;

11.5. Responder pelo cumprimento dos postulados legais vigentes de âmbito federal, estadual ou municipal, como assegurar os direitos e cumprimento de todas as obrigações estabelecidas por regulamentação, inclusive quanto aos preços praticados no contrato;

11.6. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e, inclusive, às recomendações aceitas pela boa técnica;

11.7. Implantar, adequadamente, a supervisão permanente dos serviços, de modo a obter uma operação correta e eficaz;

11.8. Prestar os serviços de forma meticulosa e constante, mantendo-os sempre em perfeita ordem;

11.9. Comunicar ao Departamento de Tecnologia da Informação do CRCMT, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários;

11.10. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com o CRCMT;

11.11. Assumir, também, a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles;

11.12. Assumir todos os encargos de possível demanda trabalhista, civil ou penal, relacionadas à execução dos serviços, originariamente ou vinculada por prevenção, conexão ou contingência;

11.13. Assumir, ainda, a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação do contrato;

11.14. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações a serem assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

11.15. Aceitar, durante a vigência do Contrato em conformidade com Art. 125 nas alterações unilaterais a que se refere o inciso I do caput do art. 124 desta Lei, o contratado será obrigado a aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato que se fizerem nas obras, nos serviços ou nas compras, e, no caso de reforma de edifício ou de equipamento, o limite para os acréscimos será de 50% (cinquenta por cento).

11.16. Fornecer, na assinatura do contrato, endereço de correspondência, telefone, e-mail e procedimentos para o encaminhamento de ofício por parte do CRCMT;

11.17. Responder, em prazo máximo de 48 horas corridas, quaisquer questionamentos realizados pelo CRCMT.

Obriga-se o CRCMT a:

11.18. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos empregados da contratada;

11.19. Assegurar-se da boa prestação dos serviços, verificando sempre o seu bom desempenho;

11.20. Assegurar-se de que os preços contratados estão compatíveis com aqueles praticados no mercado pelas demais prestadoras dos serviços objeto do contrato, de forma a garantir que lhe continuem a serem os mais vantajosos;

11.21. Controlar as ligações realizadas e documentar as ocorrências havidas;

11.22. Fiscalizar o cumprimento das obrigações assumidas pela contratada, inclusive quanto à continuidade da prestação dos serviços que, ressalvados os casos de força maior, justificados e aceitos, não devem ser interrompidas;

11.23. Solicitar, sempre que julgar necessário, a comprovação do valor vigente dos preços na data da emissão das contas mensais;

11.24. Providenciar a publicação resumida do contrato e de seus aditamentos, por extrato, na imprensa oficial.

12. DO RECEBIMENTO DOS SERVIÇOS

12.1. O objeto do contrato será recebido:

a) provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo detalhado, quando verificado o cumprimento das exigências de caráter técnico;

b) definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais;

12.1.1. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

12.1.2. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

12.1.3. Os prazos e os métodos para a realização dos recebimentos provisório e definitivo serão definidos em regulamento ou no contrato.

12.1.4 Salvo disposição em contrário constante do contrato ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

13. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

13.1. A execução dos serviços será acompanhada e fiscalizada pelo Fiscal de Contrato Vanius Joel Wojcik, que deverá, além de acompanhar e fiscalizar, atestar as Notas Fiscais/Faturas dos serviços, desde que tenham sido executados a contento, e encaminhar a documentação para pagamento.

13.2. O fiscal também deverá:

13.2.1. Notificar a empresa da intenção do CRCMT em aplicar as sanções;

13.2.2. Receber as alegações de defesa da empresa vencedora da contratada, previstas no presente termo;

13.2.3. Avaliar as alegações de defesa visando à legalidade, razoabilidade e proporcionalidade do processo;

13.2.4. Providenciar as sanções, se julgadas pertinentes, as quais serão homologadas e aplicadas pelo Ordenador de Despesa;

13.2.5. Tomar outras medidas necessárias ao fiel cumprimento da aquisição.

13.3. O contratante comunicará a contratada, por escrito, as deficiências porventura verificadas na execução dos serviços, para imediata correção, sem prejuízo das sanções cabíveis.

13.4. A presença da fiscalização do contratante não elide nem diminui a responsabilidade da contratada.

13.5. Quaisquer exigências da fiscalização, inerentes ao objeto contratual, deverão ser prontamente atendidas pela CONTRATADA, sem ônus para o CONTRATANTE.

13.6. Caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, o fiscal do contrato indicará as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.

13.7. A avaliação periódica será executada pelo Fiscal do contrato ou por outro funcionário designado pelo Conselho, no qual será o responsável pela realização da medição e avaliação.

13.8. A fiscalização técnica dos contratos avaliará constantemente a execução do objeto e utilizará *o* ***Instrumento de Medição de Resultado (IMR)***, conforme modelo previsto neste item, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

a) não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

b) deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

13.9. A utilização do **IMR** não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

13.10. A avaliação deverá ter periodicidade mensal e será baseada em indicadores, conforme as tabelas abaixo:

Tabela 1: Indicadores para mediação de resultados - IMR

Finalidade	Garantir o cumprimento das obrigações contratuais e a prestação dos serviços com qualidade
Meta a cumprir	100% dos serviços executados no modo especificado no contrato e termo de referência
Instrumento de medição	Tabela de pontuação de ocorrências
Forma de acompanhamento	Verificar as ocorrências efetuando o devido registro das mesmas para apuração total ao fim do mês
Periodicidade	Mensal
Mecanismo de cálculo	Somatório da pontuação obtida em cada ocorrência apontada dentro do período de um mês, conforme tabela de pontuação.
Inicio de vigência	Data do início da execução dos serviços
Faixas de glosa no pagamento	Até 2 pontos = 100% da fatura (não há glosa, apenas advertência) De 3 a 5 pontos = 97% da fatura (glosa de 3% sobre o valor da NF) Acima de 5 pontos = 95% da fatura (glosa de 5% sobre o valor da NF)
Sanções	Multa de 10% sobre o valor da fatura, além da glosa no pagamento, para pontuações iguais ou superiores a 10 pontos.
Finalidade	Garantir o cumprimento das obrigações contratuais e a prestação dos serviços com qualidade

Tabela 2: Tabela de pontuação de ocorrências

Item	Ocorrências	Aferição	Pontuação	Nº de ocorrências no período	Pontuação total
1	Suspender ou interromper, salvo motivo de força maior	Condicionada à verificação pelo fiscal do contrato ou à comunicação formalizada a este	3		

	ou caso fortuito, os serviços contratuais.	efetuada por funcionário que tenha verificado sua ocorrência. Os registros das ocorrências serão individuais, ou seja, a cada fato ocorrido corresponderá uma ocorrência, podendo ocorrer o registro de várias ocorrências na mesma data.			
2	Deixar de cumprir os prazos estabelecidos no contrato ou determinado pela fiscalização	Os registros das ocorrências serão individuais, ou seja, a cada fato ocorrido corresponderá uma ocorrência, podendo ocorrer o registro de várias ocorrências na mesma data.	2		
3	Problemas no atendimento à empresa e/ou usuário.	Os registros das ocorrências serão individuais, ou seja, a cada fato ocorrido corresponderá uma ocorrência, podendo ocorrer o registro de várias ocorrências na mesma data.	1		
5	Não entrega de relatórios solicitados.	Os registros das ocorrências serão individuais, ou seja, a cada fato ocorrido corresponderá uma ocorrência, podendo ocorrer o registro de várias ocorrências na mesma data.	1		
6	Ocorrências de erros, *bugs* e instabilidade nos serviços de internet sem comunicação prévia ou esclarecimentos no prazo informado.	Os registros das ocorrências serão individuais, ou seja, a cada fato ocorrido corresponderá uma ocorrência, podendo ocorrer o registro de várias ocorrências na mesma data.	2		

13.11. O relatório da medição de resultados deve ser claro e objetivo, apresentando os pontos considerados e, incluindo a documentação correspondente.

13.12. Caso a meta não seja cumprida, o relatório de medição de resultados será enviado à CONTRATADA com prazo aberto para manifestação.

13.13. As eventuais justificativas, referente às falhas apontadas devem ser encaminhadas pela CONTRATADA ao funcionário da CONTRATANTE responsável pela fiscalização do contrato.

13.14. Dirimidas as dúvidas, o fiscal do contrato formaliza o fator de qualidade ajustando o valor da medição ao IMR obtido. Com isso se obtém o valor da fatura e se configura o recebimento definitivo que autoriza a CONTRATADA a emitir a Nota Fiscal de seus serviços.

14. DO PAGAMENTO

14.1. A fatura deverá ser enviada até o 5º (quinto) dia do mês subsequente ao serviço prestado, após autorização pelo fiscal do contrato.

14.2. O pagamento deverá ser realizado em até 10 (dez) dias após o atesto da fatura pelo Fiscal do contrato.

14.3. No valor que vir a oferecer deverá ser incluído todas as despesas com taxas, fretes, enfim, todos os encargos fiscais, comerciais, trabalhistas e previdenciários, resultantes da prestação dos serviços objeto deste Procedimento.

14.4. O pagamento só será efetuado mediante consulta on-line da Regularidade Fiscal da Contratada.

14.5. A Contratante poderá deduzir do montante a ser pago os valores correspondentes a multas ou indenizações devidas pela Contratada, nos termos estabelecidos neste Termo e seus anexos.

14.6. Havendo erro na nota fiscal ou circunstância que impeça a liquidação da despesa, aquela será devolvida à contratada, e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento será de 05 (cinco) dias a iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a Contratante.

14.7. A contratante se reserva no direito de suspender o pagamento do serviço se o mesmo for efetuado em desacordo com as especificações constantes neste Edital e seus anexos.

14.8. Em cumprimento às normas e procedimentos previstos na Instrução Normativa Nº 1.234/12, expedida pela Secretaria da Receita Federal e pelas demais legislações federais, estaduais e/ou municipais o CRCMT poderá efetuar a retenção de impostos.

14.9. Não haverá a retenção dos impostos conforme descritos na Instrução Normativa Nº 1.234/12 da SRF, quando a empresa contratada for optante pelo “SIMPLES NACIONAL”, comprovada mediante entrega, juntamente com a Nota fiscal/Fatura, de documentação e de Declaração que comprove tal situação.

15. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

15.1. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

I - dar causa à inexecução parcial do contrato;

II - dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

III - dar causa à inexecução total do contrato;

IV - deixar de entregar a documentação exigida para o certame;

V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

VI - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;

X - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

XII - praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

15.2. Serão aplicadas ao responsável pelas infrações administrativas previstas nesta Lei as seguintes sanções:

I - advertência;

II - multa;

III - impedimento de licitar e contratar;

IV - declaração de inidoneidade para licitar ou contratar.

§ 1º Na aplicação das sanções serão considerados:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - as circunstâncias agravantes ou atenuantes;

IV - os danos que dela provierem para a Administração Pública;

V - a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

15.2.1. A sanção prevista no inciso I será aplicada exclusivamente pela infração administrativa prevista no inciso I do caput do art. 155 da Lei nº 14.133/2020, quando não se justificar a imposição de penalidade mais grave.

15.2.2. A sanção prevista no inciso II, calculada na forma do edital ou do contrato, não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação direta e será aplicada ao responsável por qualquer das infrações administrativas previstas no art. 155 da Lei nº 14.133/2020.

15.2.3. A sanção prevista no inciso III será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do art. 155 da Lei nº 14.133/2020, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

15.2.4. A sanção prevista no inciso IV será aplicada ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do caput do art. 155 da Lei nº 14.133/2020, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do referido artigo que justifiquem a imposição de penalidade mais grave que a sanção referida no item 12.2.3 e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

15.2.5. A sanção estabelecida no inciso IV será precedida de análise jurídica e observará as seguintes regras:

I - quando aplicada por órgão do Poder Executivo, será de competência exclusiva de ministro de Estado, de secretário estadual ou de secretário municipal e, quando aplicada por autarquia ou fundação, será de competência exclusiva da autoridade máxima da entidade;

II - quando aplicada por órgãos dos Poderes Legislativo e Judiciário, pelo Ministério Público e pela Defensoria Pública no desempenho da função administrativa, será de competência exclusiva de autoridade de nível hierárquico equivalente às autoridades referidas no inciso I deste parágrafo, na forma de regulamento.

15.2.6. As sanções previstas nos incisos I, III e IV poderão ser aplicadas cumulativamente com a prevista no inciso II.

15.2.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

15.2.8. A aplicação das sanções previstas no caput deste artigo não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

15. DA RESCISÃO DE CONTRATO

15.1. O presente contrato poderá ser extinto nas hipóteses prevista no art. 137, com consequências indicadas no art. 139, sem prejuízo das sansões previstas na lei nº 14.133/21.

15.2. Os casos de rescisão contratual serão formalmente motivados em processo administrativo instaurado para tanto, respeitado o direito constitucional a ampla defesa.

16. DA FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

16.1. A presente contratação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.

16.2. Os critérios de seleção adotados diferenciarão as propostas apresentadas e fará sobressair a proposta mais vantajosa para a Administração, respeitando o princípio da isonomia entre as licitantes.

16.2.1. Será realizada à avaliação dos preços unitários e global (12 meses) das propostas das licitantes para escolha daquela mais vantajosa, entre as propostas das proponentes habilitadas e classificadas pelo atendimento às exigências técnicas mínimas exigidas;

16.3. Para a habilitação exigir-se-á dos interessados, exclusivamente, documentação relativa a: I - habilitação jurídica; II - regularidade fiscal e III – regularidade fiscal e trabalhista.

16.4. Apresentar atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove que a empresa licitante, executou serviços com características semelhantes ao objeto do presente Termo de Referência.

17. DA VIGÊNCIA

17.1. O presente contrato vigorará pelo prazo de 12 meses, podendo ser prorrogado sucessivamente nos termos do art. 107 da Lei 14.133/21.

18. DA DEMOSTRAÇÃO DE ORÇAMENTO

18.1. Para esta contratação, serão utilizados recursos próprios do CRCMT, através do Elemento de Despesa: Programa nº 05 – Suporte e Apoio a atividades fins - Projeto nº 5002 – Tecnologia da Informação – Rubrica: 6.3.1.3.02.01.037 – Serviços de Internet.

18.2. As despesas que, eventualmente, venham a ocorrer nos demais exercícios serão custeadas com recursos previstos na Proposta Orçamentária, que serão indicados oportunamente.

19. DAS DISPOSIÇÕES GERAIS

19.1. O Conselho Regional de Contabilidade de Mato Grosso - CRCMT se reserva no direito de paralisar ou suspender, a qualquer tempo, a entrega dos serviços, mediante pagamento único e exclusivo pelos já prestados e atestados, por ajuste entre as partes interessadas.

19.2. Todos os impostos, transportes e outros aspectos financeiros deverão estar contidos nos preços da proposta comercial.

19.3. Cabe ao responsável designado pela Diretoria do CRCMT, o direito de recusar o serviço realizado que não corresponder aos critérios acima mencionados, bem como os especificados neste Termo.

19.4. A cobertura da garantia dos serviços deverá ser satisfeita pela própria contratada.

Em face ao apresentado, solicito a aquisição dos itens relacionados acima:

VANIUS JOEL WOJCIK:00004134028
Assinado de forma digital por VANIUS JOEL WOJCIK:00004134028
Dados: 2022.06.01 09:02:52 -04'00'

Vânius Joel Wojcik
Coordenador de T.I do CRCMT

Diante o exposto, autorizam a presente aquisição:

CARLOS AUGUSTO ONO GABRIEL:68872194172
Assinado de forma digital por CARLOS AUGUSTO ONO GABRIEL:68872194172
Dados: 2022.06.01 09:51:10 -04'00'

Carlos Augusto Ono Gabriel
Diretor do CRCMT

Giseli Alves Silvente
Presidente do CRCMT

Este documento foi assinado eletronicamente com fundamento no art. 4º,do Decreto nº 10.543, de 13 de novembro de 2020.

Signatários e datas conforme horário oficial de Brasília:

✔ GISELI ALVES SILVENTE (CPF XXX.666.601-XX) em 01/06/2022 12:12:22