CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

ESTUDO TÉCNICO PRELIMINAR (ETP)[1] – SOLUÇÕES DE TIC
PROCESSO ADMINISTRATIVO Nº 142/2023

Área de Negócios/Requisitante	Gerência de Tecnologia da Informação / Área de Infraestrutura – GTI/INFRA
Área Técnica (TI)	Gerência de Tecnologia da Informação – GTI
Área de Apoio Administrativo	Assessoria do Gabinete da Presidência – GAB/PRES

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	
Integrante Requisitante	Rafael Conceição da Silva, matrícula 455
Integrante Técnico	Régis de Oliveira Araújo, matrícula 1044
Integrante da Área de Apoio Administrativo	Henrique Pereira Soares, matrícula 975

1. DA DESCRIÇÃO DA NECESSIDADE

1.1. O presente ETP tem por objetivo fornecer informações necessárias para a contratação de Solução de Firewall para atendimento de necessidades relacionadas à segurança da rede corporativa do Coren-SP, tendo em vista que, em 18/09/2023, chegará ao limite legal de 60 (sessenta) meses de vigência o Contrato nº 20/2018, decorrente da Adesão nº 03/2018, relacionado ao suporte da Solução de Firewall UTM atualmente em utilização no ambiente do Coren-SP, com expiração das licenças de funcionalidades de segurança do Firewall UTM/NGFW atual (Watchguard Firebox M570) em 21/10/2023.

1.2. Adicionalmente, ainda se espera a definição de aspectos relevantes relacionados ao ambiente de conexão do Coren-SP à rede mundial de computadores, promovendo atualização de tecnologias empregadas, com o objetivo do atendimento aos melhores protocolos e padrões de qualidade de serviços, permitindo a execução da atividade finalística do órgão de maneira segura e precisa.

1.3. Tais aspectos envolvendo não apenas a substituição da solução de Firewall UTM/NGFW implantada, mas a contratação de novas soluções de segurança e conectividade que atendam as novas demandas do cenário local e mundial em termos de segurança cibernética, como a autenticação multifatorial (MFA), o modelo de segurança de confiança zero (ZTNA ou Zero Trust) e SD-WAN.

1.4. As necessidades supramencionadas são:

1.4.1. Importância de implementação de SD-WAN no cenário em que palestrantes utilizarão os links de internet das unidades descentralizadas para aulas e palestras, e onde há uma necessidade grande de economia de link de internet e administração centralizada:

a) O SD-WAN (Software-Defined Wide Area Network) é uma tecnologia que tem ganhado destaque nos últimos anos, devido a sua capacidade de oferecer uma gestão centralizada e eficiente de redes de larga escala. Essa tecnologia permite que os administradores de rede possam monitorar, gerenciar e otimizar a performance de vários links de forma centralizada, tornando a administração muito mais fácil e eficiente.

b) Além disso, o SD-WAN também permite uma economia significativa de links, já que sua tecnologia de otimização de tráfego permite que as empresas utilizem menos links para atender às suas necessidades de largura de banda. Isso significa que as empresas podem poupar dinheiro ao mesmo tempo em que aumentam a qualidade da rede.

[1] Adaptado de modelo disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/2-estudo_tecnico_preliminar_v1_2.docx (versão de 06/04/2023).

c) Outra vantagem importante do SD-WAN é a sua flexibilidade. Ele permite que as empresas escolham a opção de link mais apropriada para cada aplicação, o que pode resultar em uma melhor performance e uma maior eficiência de custo. Além disso, o SD-WAN também oferece uma gestão unificada de segurança, o que é essencial para garantir a segurança de dados sensíveis.

d) O SD-WAN é uma tecnologia fundamental para a administração centralizada e eficiente de redes de larga escala. Ele permite uma economia significativa de links, uma flexibilidade aprimorada e uma gestão unificada de segurança, tornando-o uma escolha popular para muitas empresas que buscam soluções para suas redes de dados.

1.4.2. Tendência mundial de troca da senha única para autenticação multifator (MFA) e Zero Trust[2] para evitar acesso indevido ao ambiente tecnológico do Coren-SP em caso de vazamento de senha:

a) O relatório Microsoft Digital Defense Report 2022 que destrincha os detalhes do cenário e tendências de ataques e métodos de defesa cibernética, informa que o número de ataques baseados em senha cresceu 74% em 2022, indicando uma necessidade latente de inovação e implementação de métodos que protejam as empresas de roubos de senhas, como é a solução MFA.

b) As empresas enfrentam hoje em dia diversos desafios relacionados à autenticação e senhas, tais como a segurança de informações confidenciais, a prevenção de fraudes e ataques cibernéticos, entre outros. A criação de senhas fracas e a reutilização constante de senhas são fatores que contribuem para aumentar os riscos de invasões.

c) Diante deste cenário, a implementação de uma solução contemplando o Zero Trust e a MFA se tornam fundamentais para garantir a segurança das informações armazenadas em sistemas empresariais. A MFA utiliza mais de um fator de autenticação para confirmar a identidade do usuário, tornando mais difícil para os invasores acessarem informações confidenciais.

d) Além disso, a MFA ajuda a proteger contra ameaças cibernéticas, como phishing e vishing, que visam obter informações sensíveis de usuários, tais como senhas e números de cartão de crédito. Ao adotar uma solução MFA, as empresas podem garantir que somente usuários autorizados tenham acesso a informações sensíveis e sistemas críticos.

e) Em resumo, a implementação de uma solução Zero Trust e MFA é crucial para

[2] O chamado Modelo de Segurança de Confiança Zero ou como comumente chamado, Zero Trust ou ZTNA é acrônimo do inglês '*Zero Trust Network Access*' e corresponde a uma Solução de Segurança da Informação que provê acesso remoto seguro às aplicações, dados e serviços baseados na nuvem de uma organização, a partir de políticas de controle de acessos claramente definidas. O ZTNA difere das chamadas VPNs (rede privadas virtuais) à medida que garantem acesso a serviços ou aplicações específicas definidas pelos Administradores de Rede, enquanto VPNs garantem acesso à uma rede inteira. Com um crescente número de usuários acessando recursos de organização de quaisquer lugares, soluções Zero Trust podem ajudar a eliminar gargalos identificados em outras tecnologias e métodos de acesso seguro remoto. Quanto o Zero Trust está em uso, o acesso a determinadas aplicações ou recursos são garantidos apenas depois da autenticação do usuário por meio do serviço de Zero Trust. Uma vez autenticado, a Solução Zero Trust garantirá acesso à aplicação ou serviço específico por meio da utilização de um chamado túnel criptografado, que oferece uma camada adicional de segurança, blindando aplicações e serviços de endereços IP que, salvo a camada de proteção, estariam visíveis. O ZTNA é capaz também de definir politicas de segurança para o próprio acesso a VPN e outros recursos da empresa, podendo ser utilizado em conjunto para fornecer um nível maior de segurança. Adaptado de: https://www.vmware.com/topics/glossary/content/zero-trust-network-access-ztna.html. Acesso: 14.06.2023.

garantir a segurança de informações confidenciais e prevenir ameaças cibernéticas em empresas. Além disso, é importante destacar que as empresas devem seguir práticas de segurança rigorosas, tais como a criação de senhas fortes e a não reutilização de senhas, para garantir a proteção de suas informações.

2. DA MOTIVAÇÃO/JUSTIFICATIVA DA CONTRATAÇÃO

2.1. O Coren-SP, buscando a constante melhoria e a celeridade na execução de suas atividades, necessita manter uma plataforma tecnológica atualizada e com garantia. Esta meta está incluída nos objetivos do Planejamento Estratégico 2021-2024 do programa de apoio à atividade finalística, sendo parte da atividade de ID nº 20, direcionado para a área de TI permitindo garantir a infraestrutura necessária às atividades de maneira a manter um ambiente seguro e estável com alta disponibilidade e integridade. Neste intuito, a Gerência de Tecnologia da Informação – GTI, busca manter um parque tecnológico com equipamentos atualizados, dentro da garantia e com suporte ativo.

2.2. Esta demanda prevê a contratação de Solução de Firewalls, equipamentos estes que são os principais elementos de segurança de uma rede corporativa. São eles que fazem as verificações de todas as tentativas de acesso vindas da internet. Sendo a internet conhecida como um ambiente “hostil” no que tange a segurança digital, é importante a implementação, configuração e manutenção de uma ferramenta de qualidade reconhecida e com recursos que proporcionem gerenciabilidade de elementos de segurança considerados cruciais para a Instituição. Os dispositivos UTM (Unified Threat Management), também conhecidos como Firewall UTM, são soluções do mercado de segurança digital que abrangem diversas ferramentas de segurança em um único dispositivo. Dentre essas ferramentas de segurança incluem firewall, antispam, filtro de conteúdo e proxy, antivírus de rede e IPS (Sistema de prevenção de intrusões). Esses dispositivos são conhecidos hoje por proporcionar métodos efetivos para pequenas e medias empresas conseguirem, dentre outros, gerenciar vulnerabilidades e ameaças e ao mesmo tempo reduzir custos devido à unificação de diversas ferramentas existentes. O UTM também garante que as soluções de segurança sejam compatíveis e complementares, diminuindo brechas ou falhas de segurança. Esta unificação das funções permite o gerenciamento da segurança em um único painel/console, facilitando a prevenção, detecção e ação contra ameaças de variadas fontes.

2.3. Assim sendo, a GTI busca uma solução que opere de maneira confiável, com garantia e suporte vigente para necessidades eventuais, mitigando ou diminuindo drasticamente o tempo de indisponibilidade desse item central e crítico da infraestrutura do Coren-SP, de modo a se ter a garantia de um rápido restabelecimento da comunicação dos equipamentos e computadores dependentes desse item. Tal adequação tecnológica permite ao Coren-SP seguir sua visão de futuro que, dentre outros itens, almeja ser uma autarquia reconhecida pela modernidade e comprometimento com a sociedade

3. DO ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTO

3.1. O objeto de contratação possui os seguintes alinhamentos aos instrumentos de planejamento institucionais do Coren-SP:

ALINHAMENTO AO PACC - ANO 2023	
ID	**Descrição da Contratação**
21	Contratação de Solução de Firewall

4. DAS NECESSIDADES DE NEGÓCIO

4.1. A adoção de soluções de segurança e infraestrutura integradas no ambiente das empresas é criticamente importante para garantir a segurança das informações produzidas e transitadas. Isso inclui a combinação de várias tecnologias de segurança e infraestrutura, como rede SD-WAN, firewalls, VPN,

IDS/IPS, antivírus, anti-spam, controle de acesso, MFA, Zero Trust entre outras, para proteger a rede e os dados da empresa.

4.2. Uma das principais vantagens das soluções de segurança e infraestrutura integradas é que elas oferecem uma proteção completa e abrangente para a rede da organização. Elas fornecem uma camada adicional de segurança, analisando e bloqueando pacotes maliciosos antes que eles cheguem ao sistema e permitem que a empresa implemente políticas de segurança customizadas. Isso ajuda a garantir que somente usuários autorizados tenham acesso a informações críticas e que os sistemas estejam protegidos contra ameaças cibernéticas conhecidas.

4.3. Outra vantagem, é que as soluções de segurança, quando integradas, permitem a centralização de gerenciamento de segurança, o que facilita a administração e monitoramento de todas as funções de segurança, além de fornecer relatórios e estatísticas importantes para a equipe de segurança. Ademais, as soluções de segurança integradas podem ser somadas com outras soluções, como sistemas de detecção e resposta às ameaças (EDR), o que aumenta ainda mais a segurança da rede.

4.4. Por fim, essa é uma medida de segurança importante para uma empresa, pois ela ajuda a proteger contra ameaças cibernéticas e garante que somente usuários autorizados tenham acesso a informações críticas. Isso é fundamental para proteger os interesses da empresa e garantir a confidencialidade, integridade e disponibilidade dos dados.

4.5. As soluções integradas possibilitam, sem dúvida, uma melhor visibilidade e capacidade de resposta a ameaças, o que é crucial para mitigar riscos e manter a segurança da informação.

5. DAS NECESSIDADES TECNOLÓGICAS

5.1. SD-WAN

5.1.1. A comunicação entre a unidade Sede e as unidades descentralizadas do Coren-SP, Subseções e Núcleos de Atendimento ao Profissional de Enfermagem (NAPEs) distribuídos em municípios do Estado de São Paulo é, atualmente, feita através de uma rede MPLS, com links dedicados de internet na Sede para o acesso à WEB. No entanto, a limitação de velocidade desses links tem causado gargalos na rede, implicando em dificuldades de acesso a novos serviços em nuvem, tais como e-mail e ferramentas do Microsoft 365, Solução de Comunicação e Produtividade atualmente utilizada pelo órgão. Além disso, a implementação de um sistema de monitoramento com câmeras IP de alta resolução nas subseções e NAPEs do Coren-SP tem causado lentidão na rede das unidades. Para solucionar esses problemas, é necessária a descentralização da saída de internet e adoção da tecnologia SD-WAN para garantir uma melhor qualidade de serviço e gerenciamento do tráfego de dados entre a Sede e unidades descentralizadas. Com essa mudança, cada Subseção ou NAPE terá o seu próprio link de internet, o que permitirá um maior consumo de banda e melhor desempenho na utilização dos serviços em nuvem, do sistema de monitoramento e de serviços disponíveis na internet.

5.1.2. Com a descentralização da saída de internet, é necessário garantir a segurança da rede da empresa. Por isso, será adotada uma solução de firewall centralizada que replique as regras para as filiais, possibilitando manter o controle e a segurança que temos atualmente, recurso que será adotado através da tecnologia SD-WAN.

5.1.3. Com a melhoria na conectividade, a experiência do usuário será significativamente melhorada, permitindo o acesso a novos serviços e tecnologias com maior velocidade e qualidade. Além disso, a adoção da tecnologia SD-WAN permitirá um gerenciamento mais eficiente da rede, permitindo a detecção e correção de problemas de conectividade com maior agilidade.

5.1.4. A adoção da tecnologia SD-WAN permitirá que a rede da empresa esteja preparada para o

futuro, com a possibilidade de adoção de novas tecnologias e serviços em nuvem com maior facilidade e sem prejuízo à conectividade e segurança da rede. A redundância de links na sede oferece uma camada adicional de segurança e confiabilidade, garantindo que, em caso de falha em um dos links, a rede da empresa ainda possa se manter ativa e funcionando adequadamente. Dessa forma, a empresa pode se beneficiar de uma infraestrutura de rede robusta e resiliente, capaz de lidar com as demandas e desafios do ambiente empresarial atual e futuro.

5.1.5. Além disso, a adoção da tecnologia SD-WAN permite que se tenham equipamentos nas Subseções e NAPEs que estejam preparados para eventuais necessidades futuras de implementação de links redundantes também nessas unidades.

5.2. FIREWALL (UTM/NGFW)

5.2.1. Hoje, o Coren-SP possui uma solução de firewall do tipo UTM/NGFW em operação. O vencimento iminente (outubro de 2023) das licenças de segurança desse equipamento nos leva a buscar novas soluções no mercado, e soluções adjacentes que somem à proteção do UTM/NGFW, dado que o equipamento atual e a concepção de seu projeto datam de 5 (cinco) anos atrás, quando o cenário de ameaças cibernéticas era consideravelmente menos complexo e desafiador que o cenário atual.

5.2.2. Uma Solução de firewall UTM/NGFW quando em conjunto com solução de SD-WAN permite que a empresa que possui diversas unidades descentralizadas faça um gerenciamento centralizado das configurações de políticas de segurança, liberações, bloqueios e demais configurações, ao passo que não exige que todo o tráfego de internet seja roteado pela unidade matriz da empresa, economizando banda de rede e internet.

5.2.3. A implementação de uma solução de firewall unificado (UTM/NGFW) é essencial para garantir a segurança das informações em uma empresa pública. UTM/NGFW é uma Solução que combina várias funções de segurança em uma única plataforma, incluindo firewall, VPN, IDS/IPS, antivírus, anti-spam e controle de acesso.

5.2.4. Uma das principais vantagens de uma solução firewall UTM/NGFW é que ela oferece uma proteção integrada e completa para a rede da empresa. Ele fornece uma camada adicional de segurança, analisando e bloqueando pacotes maliciosos antes que eles cheguem ao sistema e permite que a empresa implemente políticas de segurança customizadas. Isso ajuda a garantir que somente usuários autorizados tenham acesso a informações críticas e que os sistemas estejam protegidos contra ameaças cibernéticas conhecidas.

5.2.5. Por fim, a implementação de uma solução UTM/NGFW é uma medida de segurança importante para uma empresa pública, pois ela ajuda a proteger contra ameaças cibernéticas, permitindo a implementação e combinação de diversas soluções de segurança essenciais para uma rede empresarial. Isso é fundamental para proteger tanto os interesses dos cidadãos como também da própria empresa e garantir a confidencialidade, integridade e disponibilidade dos dados.

5.3. SOLUÇÃO DE AUTENTICAÇÃO MULTIFATORIAL (MFA)

5.3.1. O relatório *Microsoft Digital Defense Report 2022* [3]que destrincha os detalhes do cenário e tendências de ataques e métodos de defesa cibernética, informa que o número de ataques baseados em senha cresceu 74% em 2022, indicando uma necessidade latente de inovação e

[3] Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us. Acesso: 06.06.2023.

implementação de métodos que protejam as empresas de ataques baseados em roubo de senha ou adivinhação, como é a solução MFA.

5.3.2. A implementação de uma Solução de Autenticação Multifatorial (MFA, do inglês Multi-factor Authentication) é essencial para garantir a segurança das informações em uma empresa pública. A MFA adiciona uma camada adicional de segurança ao processo de autenticação, exigindo que o usuário forneça mais de uma forma de prova de identidade antes de ter acesso aos sistemas e dados da empresa.

5.3.3. Uma das principais vantagens da MFA é que ela ajuda a proteger contra ataques de phishing e outras táticas de engenharia social, pois exige que o usuário tenha acesso físico a um dispositivo de autenticação, como um token de segurança ou um telefone celular, além de sua senha. Isso significa que, mesmo se um invasor conseguir obter as credenciais de login de um usuário, ele ainda não será capaz de acessar os sistemas e dados da empresa sem acesso ao dispositivo de autenticação.

5.3.4. Outra vantagem da MFA é que ela permite que a empresa implemente políticas de acesso condicional, como restringir o acesso a sistemas sensíveis somente a usuários que estejam conectados a uma rede confiável ou que estejam usando um dispositivo gerenciado pela empresa. Isso ajuda a garantir que somente os usuários autorizados tenham acesso a informações críticas e que esses usuários estejam usando dispositivos seguros.

5.3.5. Assim, a implementação de uma solução de MFA é uma medida de segurança importante para uma empresa pública, pois ela ajuda a proteger contra ameaças cibernéticas e garante que somente usuários autorizados tenham acesso a informações críticas através da múltipla validação da identidade do usuário. Isso é fundamental para proteger tanto os interesses dos cidadãos como também da própria empresa.

5.4. SOLUÇÕES INTEGRADAS

5.4.1. Utilizar tecnologias do mesmo fabricante para segurança da informação de uma empresa pode trazer várias vantagens. A principal delas é a integração entre as diferentes soluções. Com tecnologias do mesmo fabricante, é mais fácil fazer com que diferentes sistemas de segurança trabalhem juntos de forma eficiente. Isso pode incluir, por exemplo, a integração entre um firewall e um sistema de detecção de intrusão, ou entre um sistema de autenticação e uma solução de gerenciamento de acesso.

5.4.2. Outra vantagem é a facilidade de gerenciamento. Se uma empresa usa tecnologias de diferentes fabricantes, pode ser necessário contratar especialistas em cada uma delas para garantir que tudo esteja funcionando corretamente. Ao escolher uma única empresa, é possível contar com especialistas que entendem como todas as soluções funcionam juntas. Além disso, esses especialistas também podem oferecer suporte e monitoramento mais rápido e eficiente em caso de problemas.

5.4.3. Além disso, usar tecnologias do mesmo fabricante pode permitir que a empresa aproveite melhor as atualizações e novas funcionalidades. Isso pode ser particularmente importante se a empresa estiver lidando com ameaças cibernéticas em constante evolução.

5.4.4. Assim sendo, as soluções de segurança de um único fabricante podem ser mais fáceis de licitar e comprar, pois a empresa tem mais facilidade para negociar e realizar a aquisição de licenças e equipamentos.

5.4.5. Em resumo, usar tecnologias do mesmo fabricante para segurança da informação de uma empresa pode trazer benefícios significativos, como integração, facilidade de gerenciamento,

melhor aproveitamento de atualizações e novas funcionalidades, e facilidade de licitação e compra.

6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

6.1. REQUISITOS DE CAPACITAÇÃO

6.1.1. Considerando a contratação de Solução ainda não implementada no ambiente do Coren-SP, torna-se necessária a capacitação de funcionários da equipe da Gerência de Tecnologia da Informação do Coren-SP (GTI) para o adequado gerenciamento dessas soluções e adequada implementação da proteção da rede. Para tanto, deverá ser fornecido treinamento para, ao menos, 6 (seis) empregados da GTI;

6.1.2. Os treinamentos deverão corresponder aos programas oficiais dos fabricantes da Solução, em termos de conteúdo e carga horária mínima.

6.1.3. Os treinamentos deverão ser ministrados por instrutores certificados pelos fabricantes das respectivas Soluções ofertadas.

6.1.4. Os treinamentos poderão ser ministrados *online* ou realizados presencialmente, na Sede do Coren-SP ou em endereço a ser indicado na cidade de São Paulo. Em quaisquer hipóteses, deverá a Contratada providenciar a infraestrutura e material que permitam o completo aproveitamento do conteúdo a ser transmitido.

6.2. REQUISITOS LEGAIS

6.2.1. Além da legislação e instruções relacionadas às contratações realizadas sob a Lei nº 14.133, de 2021, os seguintes normativos estão vinculados ao objeto desta contratação:

6.2.2. Instrução Normativa SGD/ME nº 94/2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação TIC pelos órgãos e entidades da Administração Direta do Poder Executivo Federal e adotado pelo Coren SP como boa prática;

6.2.3. Portaria Coren SP/Plenário/024/2016, de 22 de dezembro de 2016 que dispõe sobre a Política de Segurança da Informação no âmbito do Conselho Regional de Enfermagem de São Paulo;

6.2.4. A Solução ofertada deverá estar em consonância com Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

6.3. REQUISITOS DE MANUTENÇÃO E SUPORTE

6.3.1. Deverão ser ofertados pela CONTRATADA, durante todo o período de vigência contratual,[4] serviços de suporte técnico de manutenção e monitoramento para toda a Solução contratada;

6.3.2. O serviço de suporte técnico da CONTRATADA deverá ser efetuado segundo as melhores práticas do fabricante/desenvolvedor da Solução, visando sempre o máximo desempenho, disponibilidade e segurança, por técnicos devidamente certificados, de modo a garantir total interoperabilidade no ambiente computacional;

6.3.3. Os serviços de monitoramento deverão acompanhar a disponibilidade e desempenho dos ativos de TIC vinculados à solução e seus respectivos subsistemas;

6.3.4. Os serviços de monitoramento da Solução deverão ser contínuos, vinte e quatro horas por dia, sete dias por semana (24x7), produzindo análises que predigam, prevejam, previnam, detectem

[4] Por se tratar de Solução tecnológica complexa, proprietária e essencial para o funcionamento do conselho, é requisito que haja suporte e manutenção dessas soluções, para que haja respaldo da área de TI em casos de problemas, defeitos ou incidentes com a solução, por todo o período em que a mesma estará em operação no órgão.

e respondam efetivamente às ameaças, atuando proativamente como suporte de primeiro nível aos incidentes cibernéticos, monitorando o ambiente lógico da Contratante e identificando, classificando, interrompendo e catalogando todas as tentativas de ataque aos sistemas e à infraestrutura da Contratante;

6.3.5. Deverão ser executadas medidas preventivas com o objetivo de identificar e conter possíveis ataques e invasões aos ativos da Contratante.

6.3.6. Deverão ser realizadas atualizações e correções de todos os componentes da Solução ofertada durante a vigência contratual, sem ônus adicionais para a CONTRATANTE;

6.3.7. Deverão ser realizadas atualizações de versões das licenças eventualmente empregadas para operação da Solução durante toda a vigência contratual, sem ônus adicionais para a CONTRATANTE;

6.3.8. Deverão ser fornecidas novas versões corretivas ou evolutivas dos softwares, mesmo em caso de mudança de designação do nome do software, devendo compreender a correção de falhas e implementações de melhorias no produto, independentemente de correções tornadas públicas.

6.3.9. Os serviços deverão ser prestados pela CONTRATADA ou, a depender da natureza do chamado, diretamente pelo fabricante/desenvolvedor da Solução, ficando a CONTRATADA obrigada a mediar este atendimento, se necessário;

6.3.10. Os serviços de suporte incluirão o monitoramento proativo de ameaças, bem como administração das ferramentas e serviços contratados no modelo de ADMINISTRAÇÃO COMPARTILHADA.

6.3.10.1. A Administração compartilhada será entre a CONTRATANTE E CONTRATADA, considerada a seguinte definição de responsabilidades:

a) a CONTRATANTE terá autonomia para realizar alterações de configuração nos equipamentos de Firewall ofertados, com os devidos acessos e usuários administradores para login nas ferramentas de gerenciamento e relatórios;

b) a CONTRATADA também poderá realizar a configuração das ferramentas que compõem as soluções sob sua administração, a fim de garantir o uso eficiente delas;

c) A CONTRATADA deverá acionar o fabricante das ferramentas, sob sua administração, sempre que necessário, sem nenhum custo adicional para o CONTRATANTE;

d) A CONTRATADA deverá executar rotinas de monitoramento proativo nos ativos ofertados e nas funcionalidades de segurança, tomando ações de correção e combate a ameaças e notificando a CONTRATADA a respeito de casos de incidentes de segurança, ataques e outros eventos relevantes;

6.3.10.2. Considerada a divisão de responsabilidades acima definida, Matriz de Responsabilidades poderá ser elaborada e assinada entre as partes durante a implantação da Solução, compondo dos documentos que disciplinarão a execução contratual.

6.3.11. O suporte da CONTRATADA deverá disponibilizar acesso a canais de atendimento (telefônico e eletrônico) para abertura de chamados, consultas e envio de arquivos para análise durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias no ano, durante todo o período da contratação

6.3.12. Os serviços de suporte técnico à Contratante, telefônicos ou por meio de recursos de informática, deverão ser ofertados em língua portuguesa (Português 'Brasileiro').

6.3.13. Todas as formas de abertura de chamado disponíveis deverão estar efetivamente operacionais;

6.3.14. Os chamados serão classificados, em comum acordo pelas partes, de acordo com a SEVERIDADE do problema, como seguem:

NÍVEL DE SEVERIDADE	SITUAÇÃO/IMPACTO	DESCRIÇÃO
NÍVEL 1	**Situação Crítica / Sistema Indisponível**	Sistemas inoperantes ou paralisação total do ambiente.
NÍVEL 2	**Impacto Grave**	Sistemas operam com paralisação parcial do ambiente
NÍVEL 3	**Impacto Moderado**	Sistemas operam com degradação de desempenho
NÍVEL 4	**Impacto Mínimo**	Há uma necessidade de configuração adicional no ambiente / Há uma necessidade de relatório ou dúvida da equipe técnica referente ao funcionamento da Solução.

6.3.15. Os Prazos, em horas corridas, para início de atendimento e prazos para o fim do atendimento com uma solução definitiva ou de contorno são:

NÍVEL DE SEVERIDADE	PRAZO (EM HORAS CORRIDAS) PARA INÍCIO DE ATENDIMENTO (RESPOSTA) PARTIR DA ABERTURA DO CHAMADO	PRAZO (EM HORAS CORRIDAS) PARA O FIM DO ATENDIMENTO
1	1 (uma) hora	8 (oito) horas
2	2 (duas) horas	16 (dezesseis) horas
3	8 (oito) horas	16 (dezesseis) horas
4	16 (dezesseis) horas	36 (trinta e seis) horas

6.3.16. Especificamente, após a implantação dos circuitos de acesso dedicado à internet, as solicitações que envolvam solicitações de instalação, retirada e alteração de características físicas já existentes, incluindo as configurações em equipamentos de comunicação de dados decorrentes dessas mudanças, dar-se-ão através de Ordens de Serviço (OS) encaminhadas pela Contratante, sendo que estas solicitações deverão ser executadas pela Contratada em, no máximo, 30 (trinta) dias corridos contados do envio da solicitação.

6.3.17. Ao término de atendimentos de Suporte, quando solicitado pela CONTRATANTE, a CONTRATADA deverá disponibilizar Relatório de Atendimento contendo, minimamente, data e hora da abertura do chamado; data e hora do início e do término do atendimento; número de identificação do chamado; identificação do defeito ou falha na Solução; nome do funcionário da CONTRATANTE que abriu o chamado; nome do funcionário da CONTRATADA que efetuou o atendimento; descrição do problema; nível de classificação do chamado; informações sobre alteração de nível; e descrição da solução adotada e sobre a sua eficácia.

6.3.18. A CONTRATANTE poderá solicitar à CONTRATADA, ou ter acesso por meio de sítio na internet ou aplicação eletrônica a relatórios mensais referentes às solicitações de serviços, abrangendo informações **completas** dos chamados abertos e fechados, com um status para aqueles resolvidos no período.

6.3.19. A CONTRATADA deverá apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura sem custo adicional.

6.3.20. Requisitos mínimos e obrigatórios dos **SERVIÇOS DE GERÊNCIA DE REDE ENCONTRAR-SE-ÃO DETALHADOS NAS ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO.**

6.4. REQUISITOS TEMPORAIS

6.4.1. O firewall UTM/NGFW atualmente em operação no Coren-SP possui limite para licenças em 21/10/2023. Após essa data, todas as funções de segurança essenciais para a proteção da rede do Coren-SP deixarão de funcionar. Portanto, a expectativa da Administração é que os procedimentos de implantação da Solução sejam concluídos em período anterior à data crítica em questão, afastando a necessidade de ações contingenciais que possam por em risco o ambiente de rede do órgão.

6.4.2. Os serviços de Instalação e configuração da Solução compreenderão desde o início do projeto até a finalização da Implantação, que será objeto de aprovação pela Equipe Técnica da Contratante.

6.4.3. O projeto de implantação da Solução deverá contemplar todos os itens de serviços contratos, relacionados aos links dedicados de acesso à internet, SD-WAN, MFA, Zero Trust, Gerência Centralizada etc.;

6.4.4. Os cronogramas elaborados ou aprovados pelo COREN-SP, no tocante à implantação do sistema, liberações de licenças, treinamento da solução, manutenção, suporte e operação, bem como os prazos estipulados no instrumento deverão ser respeitados pela CONTRATADA;

6.4.5. O prazo máximo para conclusão do projeto é de 90 (noventa) dias corridos a partir da assinatura do contrato, conforme **CRONOGRAMA** abaixo:

CRONOGRAMA DE IMPLANTAÇÃO DA SOLUÇÃO			
ID	**AÇÕES/ETAPAS**	**RESPONSÁVEL(IS)**	**PRAZOS PARA REALIZAÇÃO/CONCLUSÃO (CONTADOS EM DIAS CORRIDOS)**
1	Reunião Inicial / Avaliação do Ambiente (a ser realizada presencialmente, na Sede da Contratante)	CONTRATANTE E CONTRATADA	Até 5 (cinco) dias corridos a partir do início da vigência contratual.
2	Apresentação de Plano de Implantação, contendo relação e cronograma das atividades de implantação da Solução, bem como disponibilização de facilitadores e canais para suporte à Contratante.	CONTRATADA	Até 10 (dez) dias corridos a partir da Reunião Inicial.
3	Aprovação do Plano de Implantação	CONTRATANTE	Até 5 (cinco) dias corridos a partir da conclusão da ação anterior.
4	Entrega das licenças da solução para conexão e proteção de usuários remotos.	CONTRATADA	Até 40 (quarenta) dias corridos a partir da aprovação do Plano de Implantação
5	Entrega e instalação dos equipamentos, links de internet dedicada e licenças que serão instalados na **Sede do Coren-SP**	CONTRATADA	Até 40 (quarenta) dias corridos a partir da aprovação do Plano de Implantação
6	Entrega e instalação dos equipamentos, links de internet dedicada e licenças que serão instalados nas **Subseções e NAPEs do Coren-SP**	CONTRATADA	Até 50 (cinquenta) dias corridos a partir da aprovação do Plano de Implantação
7	Capacitação da Equipe de TI do Coren-SP	CONTRATADA	Até 60 (sessenta) dias corridos a partir da aprovação do Plano de Implantação, mediante agendamento prévio junto à Contratante
8	Aceite da Implantação da Solução	CONTRATANTE	Até 10 (dez) dias corridos a partir da conclusão das ações 4, 5, 6 e 7
9	Entrega de relatório técnico definitivo da instalação.	CONTRATADA	Até 10 (dez) dias corridos a partir do Aceite da Implantação da Solução

10	**AUTORIZAÇÃO PARA INÍCIO DA EXECUÇÃO DOS SERVIÇOS E INÍCIO DO PERÍODO MENSAL DE FATURAMENTO**	CONTRATANTE E CONTRATADA	Os serviços de manutenção e suporte técnico da Solução se iniciarão no primeiro dia útil de execução dos serviços.

6.4.6. Os prazos do cronograma acima poderão ser ajustados de acordo com os riscos e impactos avaliados pela CONTRATANTE.

6.4.7. Os prazos definidos neste documento ou formalmente ajustados junto à Contratante deverão ser estritamente observados sob risco da aplicação de penalidades administrativas.

6.5. REQUISITOS DE SEGURANÇA

6.5.1. A CONTRATADA deverá cumprir a Política de Segurança da Informação da CONTRATANTE e assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados à CONTRATANTE, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança;

6.5.2. A CONTRATADA não poderá veicular publicidade acerca dos serviços contratados, sem prévia e formal autorização por parte da CONTRATANTE;

6.5.3. É vedado a CONTRATADA o acesso aos dados da CONTRATANTE, sem prévia e formal autorização por parte da CONTRATANTE;

6.5.4. A CONTRATADA deve comunicar formal e imediatamente a CONTRATANTE qualquer ponto de fragilidade percebido que exponha a confidencialidade, integridade ou disponibilidade das informações e do serviço;

6.5.5. A CONTRATADA deverá garantir a disponibilidade da Solução, providenciar a segurança dos dados, permitir a rastreabilidade das ações dentro do ambiente da Solução e gerenciar o tratamento de incidentes;

6.5.6. A CONTRATADA deverá manter sigilo sobre os dados e informações a que tiver acesso antes, durante e após a prestação dos serviços e garantir a mesma conduta de seu pessoal.

6.5.7. Os acessos às plataformas devem ser permitidos mediante usuário e senha.

6.5.8. As soluções ofertadas deverão possibilitar configurar o número máximo de tentativas de login no aparelho, realizando o bloqueio temporário da conta após atingir o limite de tentativas.

6.5.9. Deverão implementar criptografia em todas as comunicações que envolvam os equipamentos ou soluções ofertadas.

6.5.10. Deverão minimamente utilizar o protocolo TLS v1.2.

6.5.11. Deverão implementar mecanismos de proteção contra ataques de negação de serviço (DoS) tais como, malformed packets, oversized packets, ping floods, SYN floods e spoofing.

6.5.12. Implementar certificados digitais no tráfego TLS:

a) Conforme o padrão X.509v3;

b) Com chaves SHA256 RSA-2048Bits.

6.5.13. Deverão possuir recurso de auditoria da plataforma de forma a monitorar modificações na configuração e recursos de segurança.

6.5.14. Os requisitos de segurança para contratação de um firewall, MFA, Zero Trust e SD-WAN incluem, mas não se limitam a:

a) Capacidade de filtragem de pacotes: O firewall deve ser capaz de examinar o tráfego de rede e bloquear pacotes que não atendem aos critérios estabelecidos.

b) Suporte para protocolos de rede: Deve suportar os protocolos de rede comuns, como TCP/IP, UDP e ICMP, para que possa ser usado em diferentes tipos de redes.

c) Autenticação de usuários: O firewall deve oferecer recursos de autenticação MFA para verificar a identidade dos usuários antes de permitir o acesso à rede.

d) Controle de acesso: Deve permitir que a administração defina regras de acesso específicas para usuários, grupos e dispositivos.

e) Logs e relatórios: O firewall deve gerar logs de tráfego e relatórios para ajudar a identificar ameaças e problemas de segurança.

f) Atualizações e suporte: O firewall deve ser atualizado regularmente para corrigir falhas de segurança e receber suporte técnico para solucionar problemas e realizar monitoramento proativo.

g) Integração com outras soluções: O firewall deve ser capaz de se integrar com outras soluções de segurança, como sistemas de detecção de intrusão e antivírus, para oferecer uma proteção mais completa.

h) Alta disponibilidade: O firewall, solução MFA, Zero Trust e links devem oferecer alta disponibilidade para garantir que o serviço e a proteção estejam sempre ativos e que não cause interrupções no fluxo de trabalho da empresa.

6.6. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

6.6.1. Os softwares devem ser fornecidos em meio digital, sem a necessidade de entrega de versões dos produtos em mídias físicas;

6.6.2. Os manuais de instalação, configuração e operação de toda a Solução também deverão ser fornecidos em meio digital, com texto em língua portuguesa e/ou inglesa;

6.6.3. Os equipamentos ofertados deverão estar em conformidade com padrões estabelecidos pela Anatel para operação no Brasil e homologados pela Agência até a data de realização da licitação;

6.6.4. A documentação técnica deve ser fornecida em meio digital, com um descritivo completo do processo de implantação de cada produto ofertado, explicações sobre o registro e uso de licenças de software, forma de acesso ao site do fabricante para download, assim como de seus upgrades e updates.

6.7. REQUISITOS DE ARQUITETURA TECNOLÓGICA

6.7.1. A Solução a ser contratada deverá ser plenamente compatível com os equipamentos, softwares e soluções de TI atualmente em operação no Coren-SP, exceto o Firewall UTM/NGFW que será substituído.

6.7.2. São tecnologias de TI no Coren-SP relevantes para essa implementação:

a) Aplicações;

b) Docker;

c) Traefik;

d) Microsoft 365;

e) Azure e AWS;

f) Active Directory e

g) Serviços de terminais remotos.

6.7.3. Em relação à Sistema Operacional e Máquinas:

a) Windows Desktop (ultimas versões)

b) Tablets Android

c) Windows Server

d) Linux Debian

e) Linux Ubuntu

f) VM VMWare

g) Microsoft Hyper-V

h) Aplicações em nuvem Azure e AWS

6.7.4. Em relação à Rede:

a) Rede IPv4 e IPv6

b) VLANs

c) Roteamento

6.7.5. Os itens de serviços e componentes da Solução a ser contratada deverão ser plenamente integráveis, não podendo apresentar nenhum tipo de incompatibilidade. Para tanto, salvo alternativa técnica comprovada pela Contratada, elas deverão ser do mesmo fabricante, a fim de garantir a interoperabilidade completa entre elas, centralização das configurações, gerenciamento e relatórios.

6.8. REQUISITOS DE PROJETO E IMPLEMENTAÇÃO

6.8.1. Considerando a complexidade do projeto, que envolve a troca de equipamento central da rede do Coren-SP, a Contratada deverá apresentar plano de migração e implementação da Solução ao Coren-SP.

6.8.2. A implementação da Solução seguirá o plano de instalação/implantação apresentado pela CONTRATADA, com os prazos devidamente aprovados pelo Coren-SP.

6.8.3. A Contratada ficará inteiramente responsável pela implantação da Solução contratada, em como pelo suporte no *ongoing* (fase da execução do contrato e de garantia e suporte) em todos os casos de eventuais problemas ou necessidades de dúvidas ou correções e configurações na Solução recém entregue;

6.8.4. Os prazos para implantação e implementação dos itens de serviços e início de operação dos respectivos serviços poderão ser ajustados de acordo com as necessidades, riscos e impactos avaliados pela CONTRATANTE. Assim sendo, mediante critérios técnicos e de conveniência administrativa, a implantação poderá ocorrer de forma seriada, com formalização de demandas por meio de ordens de serviço (OS) encaminhadas pelo COREN-SP à CONTRATADA.

6.9. REQUISITOS DE IMPLANTAÇÃO

6.9.1. A Contratada deverá realizar toda a migração da Solução atualmente implantada no

Coren-SP para a Solução por ela ofertada, bem como fazer a implantação da nova Solução contratadas e sua respectiva integração no ambiente do Coren-SP, Sede e unidades descentralizadas.

6.9.2. Para a implantação em questão, as seguintes atividades serão de responsabilidade da Contratada:

a) Migração de regras de firewall do atual (interno Firebox WatchGuard e externo também Firebox WatchGuard);

b) Configurações de proteção como antispam, antivírus, application control, anti-ddos, geolocation, etc.

c) Configuração dos equipamentos na rede do Coren-SP, incluindo roteamento, Vlans, endereçamento IP, etc;

d) Configuração de perfis de navegação de internet por departamento e inspeção HTTPS;

e) VPN SSL;

f) Zero Trust, com controle de quais hosts podem ou não entrar na rede;

g) Instalação do MFA nos clientes e Integração do MFA com, minimamente:

i. Firewall contratado;

ii. Ambiente de nuvem e de colaboração;

iii. VPN SSL.

6.9.3. Todos os custos decorrentes dos processos de migração de Solução, bem como decorrentes da implantação da Solução contratada, incluindo serviços técnicos, materiais, equipamentos e eventuais deslocamentos serão de responsabilidade da CONTRATADA, devendo os respectivos custos estarem provisionados nos valores ofertados na seção de licitação, não cabendo ao Coren-SP quaisquer ônus adicionais.

6.9.4. Todos os serviços relacionados à implantação da Solução que exijam realização nas instalações da CONTRATANTE deverão ser previamente agendados, de forma a garantir o acompanhamento destes pela equipe de TI do Coren-SP, bem como para não impactar no funcionamento de atividades do órgão.

6.10. REQUISITOS DE GARANTIA

6.10.1. A Solução a ser contratada deverá estar provida de garantia durante todo o período em que estará em operação no ambiente do Coren-SP.

6.10.2. Será exigido suporte técnico para todo o conjunto de equipamentos disponibilizados, incluindo manutenção evolutiva de softwares utilizados durante todo o período de vigência contratual.

6.10.3. A garantia deverá englobar qualquer atividade relacionada à Solução contratada, tais como manutenção evolutiva, preventiva e corretiva em software. Toda a manutenção evolutiva, preventiva e corretiva ficará a cargo da CONTRATADA, sem nenhum ônus para a CONTRATANTE.

6.11. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

6.11.1. Não se aplicam ao objeto de estudos deste ETP.

6.12. REQUISITOS DE FORMAÇÃO DE EQUIPE

6.12.1. Não se aplicam ao objeto de estudos deste ETP.

6.13. REQUISITOS DE METODOLOGIA DE TRABALHO

6.13.1. Não se aplicam ao objeto de estudos deste ETP.

6.14. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

6.14.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.14.2. As informações sob custódia da CONTRATADA deverão ser tratadas como informações sigilosas, não podendo ser usadas ou fornecidas, sob nenhuma hipótese, sem autorização formal da CONTRATANTE.

6.14.3. A Solução contratada deverá possuir recursos que possibilitem a definição de regras e configurações aderentes à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD).

6.14.4. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade e que acompanhará o Termo de Referência da Contratação, deverá ser assinado pelo representante legal da Contratada no momento da contratação.

6.14.5. Ademais, acompanhando a proposta comercial deverá ser apresentada declaração de que a Contratada possui ou virá a possuir até a assinatura do Contrato, em território brasileiro, sede ou filial dotada de toda a infraestrutura técnica e de com recursos humanos qualificados e em quantidade suficiente para a prestação dos serviços de garantia aos produtos ofertados.

6.14.6. A Contratada deverá possuir processos implementados que garantem a segurança das informações da Contratante, em conformidade com a Norma ABNT NBR ISSO/IEC 27001.

7. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

7.1. A estimativa da demanda detalhada nesse tópico leva em conta o cenário atual do Coren-SP[5], bem como as necessidades específicas apresentadas, em projeção para um período de até 60 (sessenta) meses, considerado pela Equipe de Planejamento da Contratação como um ciclo de vida útil dos equipamentos de TIC adquiridos ou disponibilizados que virão a compor da infraestrutura que virá a dar suporte a qualquer que seja a solução contratada.

7.2. Equipamento virtual ou em nuvem para centralização da administração dos UTMs/NGFWs, SD-WAN, relatórios, Zero Trust e MFA:

7.2.1. Quantidade de usuários previstos para utilizar os serviços simultaneamente: 750 (setecentos e cinquenta), considerando que, em abril/2023, há 558 usuários ativos e taxa de crescimento anual de, aproximadamente, 5% (cinco por cento).

7.2.2. Considerando necessidades iniciais apuradas, porém, a quantidade mínima inicial de usuários/dispositivos para uso do MFA e Zero Trust será de 300 (trezentos), chegando até 750 ao final do período de 60 (sessenta) meses, de forma que as solicitações complementares virão a ser

[5] *Datasheet* da Solução atual de Firewall e seu quantitativo de interfaces e throughput, utilizado como base para levantamento deste ETP pode ser consultado no sítio da WatchGuard, por meio do seguinte endereço: https://www.watchguard.com/wgrd-products/appliances-compare/15021/15026/15031. Acesso: 30/05/20223.

formalizadas por meio do envio de Ordens de Serviço (OS) à Contratada.

7.3. FIREWALL TIPO 1:

7.3.1. Equipamento UTM/NGFW (atualmente o Coren-SP dispõe do Firebox M570):

7.3.1.1. 2 (duas) unidades principais para a unidade Sede do Coren-SP, de forma que seja disponibilizado um equipamento para cada segmento de rede (front-end e back-end);

a) Os equipamentos deverão incluir licença e suportar com performance aceitável para SSL VPN para pelo menos 500 usuários simultâneos no firewall externo (onde as conexões VPN serão feitas);

b) Performance (throughput mínimo) conforme Datasheet do fabricante:

I. UTM/NGFW (Full com todas as funcionalidades de segurança): 3.5Gbps;

II. IPS: 5Gbps;

III. VPN SSL: 2 Gbps;

c) Mínimo para Interfaces (fora as interfaces que eventualmente sejam necessárias para o funcionamento das conexões SD-WAN com as unidades descentralizadas (Subseções e NAPEs). Essas interfaces deverão ser entregues em conjunto com os equipamentos e deverão estar prontas para uso na entrega do objeto, incluindo eventuais licenciamentos adicionais que sejam necessários para isso:

I. 8 interfaces de 1Gb (RJ45);

II. 4 interfaces de 10Gb (fibra SFP(+) ou 8 interfaces de 1Gb (fibra SFP(+));

d) Máximo de usuários simultâneos autenticados no firewall: Sem limite de licença ou de software;

e) Máximos de sessões simultâneas no firewall: pelo menos 3 milhões;

7.4. FIREWALL TIPO 2:

7.4.1. 1 (um) equipamento do tipo UTM/NGFW para cada unidade descentralizada do Coren-SP (Subseções ou Núcleos de Atendimento ao Profissional de Enfermagem (NAPEs)) para controle de SD-WAN e políticas de segurança de cada Subseção/NAPE.

7.4.2. Esses equipamentos precisam receber e aplicar as políticas geradas numa console centralizada ou na gerência do próprio firewall da Sede. Esses equipamentos são necessários para funcionalidade do SD-WAN em cada unidade descentralizada do Coren-SP. Abaixo, segue tabela com a listagem das unidades em questão. Os referidos equipamentos deverão atender com performance satisfatória a quantidade de usuários listada, considerando uso comum da rede:

UNIDADE / ABREVIAÇÃO	ENDEREÇO	QTDE USUÁRIOS
NAPE ALTO TIETÊ - MOGI DAS CRUZES - AT	AV. VEREADOR NARCISO YAGUE GUIMARÃES, 1000 D AVÓ HIPER - POUPATEMPO - CENTRO CÍVICO - MOGI DAS CRUZES/SP	5
SUBSEÇÃO ARAÇATUBA - AR	R. JOSE BONIFACIO, 245 - CENTRO - ARAÇATUBA/SP	10
SUBSEÇÃO BOTUCATU - BOT	R. BRAZ DE ASSIS, 235 - VILA DOS LAVRADORES - BOTUCATU/SP	10
SUBSEÇÃO CAMPINAS - CA	R. SALDANHA MARINHO, 1046 - BOTAFOGO - CAMPINAS/SP	20

UNIDADE / ABREVIAÇÃO	ENDEREÇO	QTDE USUÁRIOS
SUBSEÇÃO GUARULHOS - GRU	R. MORVAM FIGUEIREDO, 65 CJ. 62 E 64 - CENTRO - GUARULHOS/SP	10
SUBSEÇÃO ITAPETININGA - ITA	R. CESARIO MOTA, 418 - CENTRO - ITAPETININGA/SP	10
SUBSEÇÃO MARÍLIA - MA	AV. RIO BRANCO, 262 - CENTRO - MARÍLIA/SP	15
SUBSEÇÃO OSASCO - OSA	R. CIPRIANO TAVARES, 130 TERREO SALA 01 - CENTRO - OSASCO/SP	10
SUBSEÇÃO PRESIDENTE PRUDENTE - PP	AV. WASHINGTON LUIZ, 300 - CENTRO - PRESIDENTE PRUDENTE/SP	10
NAPE REGISTRO – REG (AGUARDA ABERTURA)	R. ANTÔNIO POLICARPO DE SOUZA, 50 - JARDIM PLANALTO, REGISTRO - SP, 11900-000 - CENTRO - REGISTRO/SP	5 (PREVISTOS)
SUBSEÇÃO RIBEIRÃO PRETO - RP	AV. AVENIDA PRESIDENTE VARGAS, 2001 CJ. 194 - JD STA ANGELA - RIBEIRÃO PRETO/SP	15
NAPE SANTA CECÍLIA - SC	R. RUA DONA VERIDIANA, 298 - SANTA CECÍLIA - SÃO PAULO/SP	20
NAPE SANTO AMARO - AMR	R. AMADOR BUENO, 328 SALA 1, TERREO - SANTO AMARO - SÃO PAULO/SP	5
SUBSEÇÃO SANTO ANDRÉ - AND	R. DONA ELISA FLAQUER, 70 3 ANDAR, SALAS 31,36 E 38 - CENTRO - SANTO ANDRÉ/SP	10
SUBSEÇÃO SANTOS - SS	AV. DOUTOR EPITACIO PESSOA, 214 - BOQUEIRÃO - SANTOS/SP	15
SUBSEÇÃO SÃO JOSÉ DO RIO PRETO - ST	AV. ALBERTO ANDALÓ, 3764 - VILA REDENTORA - SÃO JOSÉ DO RIO PRETO/SP	10
SUBSEÇÃO SÃO JOSÉ DOS CAMPOS - SJ	AV. DR. NELSON D AVILA, 389 SALA 141 A - CENTO - SÃO JOSÉ DOS CAMPOS/SP	10
NAPE SOROCABA - SOR	AV. WASHINGTON LUIZ, 320 TÉRREO LOJA EXTERNA 03 - JARDIM EMÍLIA - SOROCABA/SP	5

7.5. Links de Internet Dedicada

Internet Dedicada

7.5.1. Em relação aos serviços de acesso dedicado à internet, com velocidades de 100 (cem) e 300 (trezentos) Mbps, destinados à Sede e unidades descentralizadas do Coren-SP, de acordo com demandas de cada localidade, especialmente em relação à quantidade de público atendido e quantidade de empregados, no caso das unidades descentralizadas, a Gerência de TI do Coren-SP estimou o seguinte dimensionamento:

UNIDADE	QUANTIDADE DE LINKS ATIVOS	BANDA (Mbps)
Alto Tietê Mogi das Cruzes – MOGI	1	100
Araçatuba – ARA	1	100
Botucatu – BOT	1	100
Campinas – CAM	1	100
Guarulhos – GRU	1	100
Itapetininga – ITA	1	100
Marília – MAR	1	100
Matriz – SP (links principal e redundante)	2	300
Osasco – OSA	1	100
Presidente Prudente – PP	1	100
Registro – REG (AGUARDA ABERTURA)	1	100

UNIDADE	QUANTIDADE DE LINKS ATIVOS	BANDA (Mbps)
Ribeirão Preto – RP	1	100
Santa Cecília – SC	1	100
Santo Amaro – AMR	1	100
Santo André – AND	1	100
Santos – SAN	1	100
São José do Rio Preto – SJRP	1	100
São José dos Campos – SJC	1	100
Sorocaba – SOR	1	100

7.6. O detalhamento completo dos requisitos técnicos da Solução como um todo seguem disponíveis no Apenso II – Requisitos Técnicos da Solução.

7.7. O NAPE Registro, previsto no objeto inicial de contratação, corresponde a uma unidade do Coren-SP que se encontra em processo de planejamento de abertura, porém sem data de inauguração definida. Considerando, porém, que se trata de contratação programada, esta se encontra prevista de forma a levar ao conhecimento da Contratada a obrigação de atendê-la, quando solicitado pelo Coren-SP. Neste caso, a ativação da Solução no futuro Nape Registro dependerá de prévia formalização da Contratante, a ser encaminhada à Contratada por meio do envio de Ordem de Serviço (OS).

8. LEVANTAMENTO DE SOLUÇÕES

A – LEVANTAMENTO DE SOLUÇÕES DISPONÍVEIS

8.1. NECESSIDADES SIMILARES EM OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA E AS SOLUÇÕES ADOTADAS

8.1.1. A tabela abaixo ilustra algumas contratações realizadas pela Administração relacionadas com o objeto de estudos deste ETP e utilizadas, pela Equipe de Planejamento da Contratação, como fonte de informações para construção da descrição da Solução a ser contratada:

UASG	ÓRGÃO	SOLUÇÃO	PREGÃO	DESCRITIVO DO OBJETO
925099	PMSP - EMPRESA DE TEC. DA INFORMAÇÃO - PRODAM	UTM/ NGFW	9002/2022	Locação de solução de segurança composta de Firewall Appliance incluindo sistema de segurança do tipo IPS, Gateway Anti-Malware, Filtro de Conteúdo, Controle de Aplicação, licenças e demais serviços previstos no Termo de Referência, por 36 meses, conforme condições e especificações constantes no Edital e seus Anexos.
70013	TRIBUNAL REGIONAL ELEITORAL DA BAHIA	MFA	47/2022	Registro de preços para eventual contratação de serviço de autenticação por múltiplos fatores, com fornecimento de tokens homologados, serviço de instalação com repasse de conhecimento e treinamento oficial do fabricante
495130	COMPANHIA DE PESQUISA DE RECURSOS MINERAIS	MFA	35/2022	Contratação de empresa para fornecimento de Solução de Acesso Remoto Seguro, autenticado e autorizado às aplicações empresariais exclusivamente através de nuvem no formato SaaS para funcionários, parceiros, terceiros, prestadores de serviços e/ou fornecedores. Deverão ser fornecidas licenças de uso (subscrição) para até 1000 (mil) usuários, incluindo os serviços de configuração, ativação e suporte técnico, pelo período de 36 (trinta e seis) meses.
927045	TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ	UTM/ NGFW	jan/21	Contratação de empresa especializada para o fornecimento de Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças (Firewall UTM/NGFW) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall); Solução de software para gerenciamento de logs e eventos de segurança (SIEM - Security Information and Event Management), além de suporte técnico e serviços especializados.

UASG	ÓRGÃO	SOLUÇÃO	PREGÃO	DESCRITIVO DO OBJETO
110120	DEPARTAMENTO DE ADMINISTRACAO DA ABIN/GSI/PR	UTM/ NGFW	45/2019	Solução de proteção de rede, com características de Next Generation Firewall (NGFW), incluindo filtro de pacotes, reconhecimento e controle de aplicação, administração de largura de banda (QoS) e roteamento dinâmico por aplicação, redes privadas virtuais (VPN) IPSec e SSL, descriptografia de tráfego SSL/TLS, sistema de prevenção a intrusão (IPS) contra ameaças cibernéticas de vírus, spywares e malwares Zero Day , filtro de URL, autenticação de duplo fator, console de gerenciamento com interface integrada à plataforma de inteligência de ameaças do mesmo fabricante; plataforma integrada de inteligência de ameaças e Emulador local de artefatos suspeitos (on-premises sand-box appliance), compondo uma plataforma de segurança integrada e de alta disponibilidade
925468	TRIBUNAL DE CONTAS DO EST.DO R.G. DO NORTE	UTM/ NGFW	13/2013	Aquisição de Soluções de Segurança FIREWALL (UTM/NGFW e WAF), voltadas para o atendimento das necessidades do Tribunal de Contas do Estado do Rio Grande do Norte, de acordo com as quantidades e especificações técnicas constantes da Relação de Bens Especificações Técnicas - Anexo II do Edital.
90031	TRIBUNAL REGIONAL FEDERAL DA 5ª REGIAO	MFA	51/2012	Registro de Preços para a aquisição de licença do sistema de autenticação de dois fatores da RSA Authentication Manager e tokens OTP (One Time Password) em hardware e software, e, suporte técnico on-site.
153978	MEC/INEP/INST.NAC.DE EST.E PESQ.EDUCAC./DF	MFA	22/2012	Aquisição de solução de segurança de autenticação forte que se baseia na tecnologia conhecida como Segundo Fator de Autenticação através de senha dinâmica OTP One Time Password, onde toda a infraestrutura da solução ficará hospedada no ambiente seguro físico e lógico do INEP, contemplando: software, instalação, entrega de APIs e Web Service, suporte técnico e atualização de versões, bem como transferência de tecnologia da solução.
100001	TRIBUNAL DE JUSTICA DO DISTRITO FEDERAL	SD-WAN	63/2022	Contratação de prestação de serviços de rede corporativa de longa distância (WAN), composta por acessos MPLS e Internet, com fornecimento de equipamentos SD-WAN do tipo appliance, para a interligação dos Datacenters do TJDFT a seus fóruns e pontos de presença, englobando instalação, configuração de equipamentos e enlaces de comunicação e gerenciamento proativo contra falhas, por 30 meses, nos termos do edital e dos seus anexos.
928680	NAV BRASIL SERVIÇOS DE NAVEGACÃO AEREA S.A.	SD-WAN	fev/23	Seleção de proposta mais vantajosa para a contratação de empresa especializada no fornecimento de soluções de conectividade baseadas na internet (links de dados de longa distância) e de soluções de SD-WAN (Software Defined Wide Area Network, incluindo o fornecimento, instalação, configuração, monitoramento, gestão das soluções, suporte e garantia de equipamentos, para atendimento à Administração Central e dependências da NAV Brasil em âmbito nacional.
130005	COORD.-GERAL DE EXECUCAO ORÇ.E FIN./DA/MAPA	SD-WAN	22/2022	Solução corporativa de comunicação de dados capaz de prover conexão com Internet e interconexão da sede do Ministério da Agricultura, Pecuária e Abastecimento - MAPA e suas unidades regionais de acordo com as características, quantitativos e especificações contidas no Edital e seus anexos.
925509	TRIBUNAL DE JUSTIÇA DO ESTADO DO ACRE	UTM/ NGFW / SD-WAN	58/2021	Contratação de empresa especializada para 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.
989185	PREFEITURA MUNICIPAL DE TANGARA DA SERRA	UTM/ NGFW / SD-WAN	49/2021	CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PROMOVER A CONECTIVIDADE ENTRE O AS (AUTONOMOUS SYSTEM) DA PREFEITURA DE TANGARÁ DA SERRA E A REDE MUNDIAL DE COMPUTADORES COM SOLUÇÃO INTEGRADA DE SEGURANÇA (ANTI-DDoS E FIREWALL UTM/NGFW SD-WAN), para atender a demanda das secretarias, conforme especificações contidas no Termo de Referência e demais exigências estabelecidas neste Edital e seus anexos
70018	TRIBUNAL REGIONAL ELEITORAL DE SAO	SD-WAN	114/2020	Pregão Eletrônico - REGISTRO DE PREÇOS para contratação de serviços de telecomunicações para provimento da comunicação de dados do TRE/SP

UASG	ÓRGÃO	SOLUÇÃO	PREGÃO	DESCRITIVO DO OBJETO
	PAULO			(Backbone Secundário),

8.2. ALTERNATIVAS DO MERCADO

8.2.1. Dentre as alternativas de mercado, para atendimento das necessidades de negócio manifestadas, a EPC identificou os seguintes cenários:

CENÁRIO 1 - COMPRA DE EQUIPAMENTOS E LICENÇAS DE FIREWALL UTM/NGFW, ZERO TRUST E MFA COM CONTRATO DE SUPORTE E GARANTIA: É a alternativa mais direta, onde o Coren-SP detém controle total da Solução. É o cenário atual no Coren-SP para o Firewall UTM/NGFW e que oferece maior agilidade no atendimento de demandas novas e correções de problemas. Esse modelo, porém, não possui monitoramento 24x7 por parte do fornecedor tampouco as vantagens do SD-WAN, que é a descentralização dos acessos e configurações de links de internet por política.
CENÁRIO 2 - ALUGUEL DE EQUIPAMENTOS FIREWALL UTM/NGFW, ZERO TRUST E MFA E LICENÇAS COM CONTRATO DE SUPORTE E GARANTIA: Este cenário varia em termos de valores em relação ao Cenário 1, tendo em vista não exigir investimento inicial de maior monta. Tal modelo, porém, apresenta as mesmas desvantagens identificadas no cenário 1, tais como não possuir monitoramento 24x7 do fornecedor e não possuir as vantagens do SD-WAN.
CENÁRIO 3 - CONTRATAÇÃO DE SD-WAN, FIREWALL UTM/NGFW, MONITORAMENTO, ZERO TRUST E MFA COM ADMINISTRAÇÃO COMPARTILHADA ENTRE A CONTRATADA E CONTRATANTE JUNTAMENTE COM CONTRATAÇÃO DE LINKS DE INTERNET PARA A SEDE, SUBSEÇÕES E NAPES Contratação de empresa fornecedora de SD-WAN, com administração compartilhada das soluções de segurança, monitoramento 24x7 das soluções de segurança e treinamento das soluções. É o modelo que melhor atende os requisitos de negócio e tecnológicos definidos pelo Coren-SP, permitindo a administração compartilhada das soluções de segurança, a partir da definição de uma matriz de responsabilidades entre Contratante e Contratada.. Tal modelo permitirá a autonomia nas configurações e análises de segurança e rede do ambiente do Coren-SP pela equipe de TI do órgão com o respaldo de um fornecedor acompanhando os eventos de rede e segurança em modelo 24x7. Dado que o Coren-SP possui profissionais de TI qualificados para administração de rede, firewall e soluções de segurança, a princípio, se entende que essa é a melhor alternativa para esse tipo de objeto.

8.3. EXISTÊNCIA DE SOFTWARE PÚBLICO BRASILEIRO (QUANDO APLICÁVEL)

8.3.1. Não se aplica para o objeto de estudos deste ETP.

8.4. POLÍTICAS, OS MODELOS E OS PADRÕES DE GOVERNO (A EXEMPLO DO EPING, EMAG, EPWG, ICP-BRASIL E E-ARQ BRASIL, QUANDO APLICÁVEIS)

8.4.1. Não se aplica para o objeto de estudos deste ETP.

8.5. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO OU ENTIDADE PARA VIABILIZAR A EXECUÇÃO CONTRATUAL (A EXEMPLO DE MOBILIÁRIO, INSTALAÇÕES ELÉTRICAS, ESPAÇO ETC.)

8.5.1. Não haverá necessidade de adequações significativas no ambiente de TI do Coren-SP dado que qualquer Soluções contratada se adequará às necessidades do órgão, demandando ajustes pontuais de rede e de configurações que não impactam no Coren-SP, sendo os ajustes em questão comuns em qualquer migração de infraestrutura de TI.

8.5.2. A Solução a ser contratada, entendida pelo Cenário C, porém, tratará de substituir alguns contratos atualmente vigentes para infraestrutura de TI, que são identificados abaixo:

Rede MPLS: Contrato nº 13/2021, decorrente do PE nº 07/2021. Motivo: Remodelagem e modernização do padrão de conexão para melhoria da segurança, conectividade e experiência dos usuários nas unidades. As novas tecnologias utilizadas e aquelas previstas para o futuro próximo (como videoconferências) demandam uma nova necessidade em termos de segurança e desempenho da rede.
Links WAN: Contrato nº 25/2022, decorrente do PE nº 27/2022. Motivo: Remodelagem e modernização do padrão de

conexão para melhoria da segurança, conectividade e experiência dos usuários nas unidades. As novas tecnologias utilizadas e aquelas previstas para o futuro próximo (como videoconferências) demandam uma nova necessidade em termos de segurança e desempenho da rede.
Firewall: Contrato nº 20/2018, decorrente da AD nº 03/2018. Motivo: Além dos mesmos motivos tratados nos demais pontos (MPLS e WAN), há o vencimento iminente das licenças das proteções dos Firewalls atualmente contratados, o que demanda uma nova contratação dado que não é mais possível renovar esse contrato além do limite legal de 60 meses definido pelo art. 57, II da Lei nº 8.666/1993.

8.5.3. Desta forma, a Gerência de TI, fiscais e gestor contratuais deverão estabelecer **plano de desmobilização dos contratos vigentes**, de forma que a transição contratual não represente risco ao Coren-SP, tendo em vista que o acesso à internet é requisito ***indispensável*** para a manutenção das atividades finalísticas e administrativas da instituição.

8.6. POSSIBILIDADE DE AQUISIÇÃO NA FORMA DE BENS OU CONTRATAÇÃO COMO SERVIÇO

8.6.1. Considerando os requisitos de negócio e tecnológicos apresentados, tem-se que as necessidades da Administração como um todo não poderiam ser supridas por meio da aquisição exclusiva de equipamentos *firewall*, ainda que acompanhados de manutenção preventiva e corretiva, tendo em vista que o objeto da contratação acoberta serviços relacionados a links SD-WAN, à Solução de Segurança da Informação prestação de Serviços de Segurança de Perímetro realizadas por empresas especializadas, compreendendo o fornecimento, instalação, suporte técnico, garantia, monitoramento 24x7 e o treinamento de sistemas de: Firewall de UTM/NGFW (com Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway) e MFA.

8.6.2. A Contratação de serviços conforme descritos no cenário '3' é prática comum de mercado, de forma que a EPC identificou a existência de mercado fornecedor no Estado de São Paulo que poderá atender às demandas manifestadas pelo Coren-SP na modalidade de serviços.

8.7. DIFERENTES TIPOS DE SOLUÇÕES EM TERMOS DE ESPECIFICAÇÃO, COMPOSIÇÃO OU CARACTERÍSTICAS DOS BENS E SERVIÇOS INTEGRANTES

8.7.1. As soluções apresentadas neste estudo deverão atender as necessidades do COREN-SP e contemplar as exigências descritas no Apenso II – Requisitos Técnicos da Solução.

8.8. AMPLIAÇÃO OU SUBSTITUIÇÃO DA SOLUÇÃO IMPLANTADA

8.8.1. Da Eventual Ampliação da Solução Contratada

8.8.1.1. O dimensionamento da Solução realizado pela área técnica/requisitante, GTI, considera o atendimento das necessidades atuais do órgão, projetando-o para um período de 60 (sessenta) meses.

8.8.1.2. Porém, no decorrer da execução contratual, mediante virtualização de serviços e/ou surgimento de demandas que exijam maior largura de banda para conexão, que até então não são objeto de previsão no ambiente da instituição, mediante aditamento contratual, respeitados as condições de alteração contratual permitidas pela Lei nº 14.133/2021, poderão ser viabilizados aumentos de bandas contratadas.

8.8.1.3. Ainda, considerada a possibilidade de alteração de endereços ou abertura de unidades do Coren-SP em municípios do Estado de São Paulo, previstos ou não previstos no objeto de contratação inicial, fica estabelecido que o Coren-SP poderá solicitar alterações de endereços de instalação ou novas instalações de links e equipamentos destinados a novas unidades, neste caso respeitados os limites de alteração contratual definidos na Lei nº

14.133/2021.

8.8.1.4. Para tanto a Contratada deverá prover a infraestrutura necessária para a instalação desses itens nos locais indicados, bem como a extensão do ambiente e configuração para os mesmos.

8.8.1.5. A Contratada não poderá alegar desconhecimento desse fato no momento da contratação, sendo que somente ficará desobrigada desse serviço caso apresente laudo técnico comprovando a impossibilidade técnica de instalação dos links, equipamentos ou serviços na localidade indicada pela Contratante.

8.8.1.6. As alterações de endereço de instalação e/ou de acréscimo de localidades ao objeto de contratação serão objeto de Termo Aditivo.

8.8.2. Da Substituição da Solução Contratada

8.8.2.1. Ao término da relação contratual, seja por motivos de término de vigência ou rescisão, caberá à Contratada a retirada de todos os equipamentos disponibilizados à Contratante em regime de comodato e que foram necessários à operação da Solução como um todo.

8.9. DIFERENTES MÉTRICAS DE PRESTAÇÃO DO SERVIÇO E DE PAGAMENTO

8.9.1. Conforme observado, verificou-se que as modalidades dos pagamentos das contratações similares realizadas por outros órgãos ou entidades da administração pública possuem em sua maioria a mesma métrica de prestação do serviço com pagamento mensal.

B – IDENTIFICAÇÃO DAS SOLUÇÕES

ID	DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO)
1	**Compra de equipamentos e licenças de Firewall UTM/NGFW, Zero Trust e MFA com contrato de suporte e garantia**. É a alternativa mais direta, onde o Coren-SP detém controle total da solução. É o cenário atual no Coren-SP para o Firewall UTM/NGFW e que oferece maior agilidade no atendimento de demandas novas e correções de problemas. Esse modelo não possui monitoramento 24x7 do fornecedor e não possui as vantagens do SD-WAN (descentralização dos acessos e configurações de links de internet por política).
2	**Aluguel de equipamentos Firewall UTM/NGFW, Zero Trust e MFA e licenças com contrato de suporte e garantia**: Esse cenário varia em termos de valores para o modelo 1. Apresentando assim as mesmas desvantagens administrativas das soluções. Como não possuir monitoramento 24x7 do fornecedor e não possuir as vantagens do SD-WAN (descentralização dos acessos e configurações de links de internet por política).
3	**Contratação de SD-WAN, Firewall UTM/NGFW, Zero Trust e MFA com administração compartilhada entre a CONTRATADA e CONTRATANTE:** Contratação de empresa fornecedora de **SD-WAN**, com **administração compartilhada** das soluções de Segurança, **monitoramento 24x7** das soluções de segurança e Treinamento das Soluções. Esse modelo deve possuir uma matriz de responsabilidades, definindo onde cada parte atua e o que cada uma pode ou não fazer nos ativos contratados. É o modelo que reúne o melhor dos mundos da contratação de empresa para administração sem perdermos a autonomia nas configurações e análises de Segurança e Rede do ambiente do Coren-SP. Nesse modelo temos o respaldo de um fornecedor olhando os eventos de rede e segurança em modelo 24x7, ao passo que mantemos nossa autonomia de administração do ambiente. Dado que o Coren-SP possui profissionais de TI qualificados para administração de rede, firewall e soluções de segurança, entende-se que essa é a melhor alternativa para esse tipo de objeto.

9. ANÁLISE COMPARATIVA DE SOLUÇÕES/CENÁRIOS

9.1. De forma a permitir a identificação de soluções/cenários viáveis para o atendimento das necessidades da Administração, o quadro abaixo se propõe a comparar as diferentes soluções/cenários

identificados em relação aos requisitos da contratação:

REQUISITO	SOLUÇÃO/ CENÁRIO	SIM	NÃO	N/A
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1, 2 e 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	1, 2 e 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	1, 2 e 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	1, 2 e 3			X
A Solução é aderente às regulamentações da ICP-Brasil?	1, 2 e 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1, 2 e 3			X

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

10.1. SOLUÇÃO INVIÁVEL 1: CENÁRIO 1 - Compra de equipamento de Segurança sem SD-WAN.

10.1.1. Tratando-se do cenário em que o Coren-SP atualmente se encontra inserido, a partir da experiência do próprio órgão, se é possível observar que a contratação de serviços de TI, em detrimento à aquisição de equipamentos pode ser uma escolha mais vantajosa para melhor atendimento das necessidades atuais e futuras do órgão. Dentre outras, sem prejuízo do menor investimento inicial, são enumeradas abaixo algumas razões técnicas pelas quais a contratação de serviços pode ser a melhor opção:

10.1.1.1. Atualizações constantes: As tecnologias de TI estão sempre evoluindo, e equipamentos rapidamente ficando obsoletos. Na contratação de Soluções de TI como serviços, é possível o acesso das contratantes às tecnologias mais recentes, processo facilitado por previsões contratuais que exijam a constante atualização das soluções. No caso de aquisições, especialmente quando pensado em termos de contratações públicas, não se é possível imprimir às aquisições ritmo alinhado com a atualização de tecnologias, o que pode, inclusive, tornar suscetível o órgão às novas ameaças não monitoradas por soluções implantadas, quando se fala de soluções relacionadas à segurança da informação;

10.1.1.2. Suporte técnico: Empresas especializadas em serviços de TI dispõem de equipes de suporte técnico altamente capacitadas, voltadas ao atendimento de chamados e ordens de serviço dentro das melhores práticas dos fabricantes. Ademais, prestam-se à resolução de problemas dentro de níveis de serviços (SLAs) estabelecidos em contrato, sob hipótese de glosas ou aplicação de penalidades administrativas nas hipóteses de descumprimentos de SLAs. A contratação de serviços de TI com suporte técnico incluso, ademais, permite à equipe de TI da contratante empregar esforços em atividades diretamente relacionadas a objetivos da organização, tendo em vista que passarão a acompanhar os serviços meio da posição de gestores contratuais;

10.1.1.3. Mitigação de riscos: Na contratação de Soluções de TI enquanto serviços, é contratualmente formalizada a responsabilidade da sustentação dos ambientes e operação dos sistemas para uma empresa especializada contratada. Em outras palavras, mantidos cuidados relacionados ao acompanhamento da execução contratual, de responsabilidade da Contratante, transferem-se processos para agente com maiores

recursos para resolução de problemas – no caso da presente contratação, relacionados à redução de riscos de problemas de segurança ou perda de dados.

10.1.2. Resumidamente, a contratação de Soluções de TI como serviço, do ponto de vista técnico, é considerada alternativa flexível e mais segura do que a compra de equipamentos. Além disso, permite uma menor carga para TI, retirando a preocupação com a manutenção e atualização dos sistemas em questão.

10.1.3. Adicionalmente, esse modelo não contempla **aspecto crítico** vislumbrado pela equipe de TI do Coren-SP, que é a tecnologia SD-WAN e todos os seus benefícios já citados anteriormente.

10.1.4. Cumpre destacar que as Soluções SD-WAN comercializadas em mercado envolvem a disponibilização de equipamentos, uma vez que o gerenciamento e monitoramento de rede, proporcionado pelos equipamentos e softwares, fazem parte do escopo das referidas Soluções.

10.2. SOLUÇÃO INVIÁVEL 2: CENÁRIO 2 - Aluguel de equipamento de Segurança sem SD-WAN.

10.2.1. A contratação de Solução de TI como serviço, no caso de serviços comuns, é uma alternativa mais viável do que a aquisição de equipamentos de TI em diversos aspectos. Dentre outras, são enumeradas abaixo algumas razões pelas quais a terceirização de TI é entendida como alternativa tecnicamente recomendável e que, pelas vantagens produzidas, também que proporciona maior economicidade:

10.2.1.1. Menor investimento: Ao terceirizar os serviços de TI, dentro do modelo de contrato que acoberta demandas requisitadas por meio de ordens de serviço, a contratante paga apenas por serviços que precisa, afastando, ademais, gestão de contratos de manutenção ou investimentos intermediários com a atualização de equipamentos. Ademais, na contratação de Solução de TI como serviço, há a previsão de atualização de licenças de software que, em muitas hipóteses, corresponde a contratação apartada do hardware;

10.2.1.2. Especialização: Empresas especializadas em serviços de TI possuem profissionais altamente especializados e treinados nas últimas tecnologias e tendências do setor, podendo fornecer soluções personalizadas e eficientes que atendam às necessidades específicas das contratantes;

10.2.1.3. Escalabilidade: A contratação de Solução de TI como serviço permite ao cliente o ajuste do nível de suporte de TI de acordo com necessidades presentes. Isto é, dentro de um cenário de contratação perdurando, no caso da Administração Pública até 60 (sessenta meses), a organização pode prever cláusulas contratuais que atendam ao crescimento de demandas, sem proporcionar investimento superdimensionado em relação às necessidades iniciais da contratante;

10.2.1.4. Maior flexibilidade: A contratação de serviços permite, na hipótese de agravamento de níveis de serviços, maior flexibilidade na troca de fornecedor ou de tecnologia, movimento agravado quando se vislumbra parque tecnológico próprio. Dentro da Administração Pública abundam exemplos, especialmente em contratações de TI, de Soluções que, quando finalmente adquiridas, já são obsoletas em relação às tecnologias ou práticas de mercado.

10.2.2. Desta forma, importa consignar que o Cenário 2, comportado, de certa forma, dentro do Cenário 3, é considerado inviável em função de tratar da locação de equipamentos de segurança sem a tecnologia SD-WAN e todos os seus benefícios já citados anteriormente. A EPC, em tempo, identificou que há mercado de fornecedores que ofertam soluções completas envolvendo serviços

de **SD-WAN, Firewall UTM/NGFW, Zero Trust e MFA com administração compartilhada entre a CONTRATADA e CONTRATANTE, correspondendo ao Cenário 3, entendido como a Solução viável pela Equipe de Planejamento da Contratação.**

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

11.1. Da Metodologia da Pesquisa Estimativa de Custos das Soluções/Cenários Viáveis

11.1.1. A pesquisa estimativa de custos da Solução considerou ou parâmetros definidos na IN SEGES/ME nº 65/2021, especialmente com a utilização de referências obtidas de pesquisas juntos a fornecedores especializados e valores de contratações similares da Administração, parâmetros IV e II do art. 5º da referida Instrução Normativa de pesquisa de preços.

11.2. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE – CENÁRIO 3

11.2.1. Tratando-se, pois, do Cenário 3, contemplando a **contratação de Solução que envolva serviços de SD-WAN, Firewall UTM/NGFW, monitoramento, Zero Trust e MFA**, foram solicitados a fornecedores especializados que cotassem os serviços considerando um período de 12 (doze) ou 60 (sessenta) meses. Tais levantamentos objetivaram a verificação da existência de maior vantagem econômica decorrente da contratação plurianual, considerando que se trata de diretriz definida no inciso I do art. 106 da Lei nº 14.133/2021 para a contratação de serviços contínuos pelo prazo de até 5 (cinco) anos nas hipóteses de serviços contínuos, o que é o caso do presente objeto, tendo em vista a imprescindibilidade da conexão segura à rede mundial de computadores para o funcionamento de quaisquer atividades finalísticas ou administrativas do órgão.

11.2.2. Assim posto, a tabela do **Apenso I deste ETP – Comparativo dos Custos Totais de Propriedade – TCO** demonstrou economicidade mínima da ordem de 5,45% (cinco inteiros e quarenta e cinco décimos por cento) quando comparadas as contratações do Cenário 3 com vigência inicial de 12 (doze) e 60 (sessenta) meses, demonstrando, *sem prejuízo da economicidade operacional e administrativa relacionada à contratação plurianual*, a existência de vantajosidade *a priori* da contratação plurianual.

11.3. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

11.3.1. O quadro abaixo representa estimativa de gastos máximos para o período de 60 (sessenta) meses considerado o consumo máximo dos itens de serviços contemplados no Cenário 3, cujos valores unitários, obtidos da pesquisa estimativa de preços realizada pela Equipe de Planejamento da Contratação, encontra detalhamento no quadro do subitem 13.1 abaixo.

11.3.2. Importa destacar que a contratação da Solução não exigirá a realização de outros investimentos por parte da Administração, relacionados à contratação de pessoal, arranjos de estrutura ou realização de contratações correlatas. Assim sendo, o TCO da contratação corresponderá à evolução de um único contrato dentro de um período de 60 (sessenta) meses, já entendida a vantagem econômica decorrente da contratação plurianual. Em relação ao índice inflacionário considerado para o período, a EPC utilizou do IST – Índice de Serviços de Telecomunicações[6], índice setorial mantido pela Anatel, aplicado ao mercado de telecomunicações (considerando que os links dos tipos 1 e 2 correspondem à parcela de maior valor do objeto final).

DESCRIÇÃO	ESTIMATIVA DE TCO AO LONGO DOS ANOS[7]	TOTAL

[6] Disponível em: https://www.gov.br/anatel/pt-br/regulado/competicao/tarifas-e-precos/valores-do-ist. Acesso: 13.06.2023.

[7] Importante destacar que o TCO corresponde a uma estimativa de valor máximo a ser empenhado pela Administração considerada a correção dos valores contratados em todos os períodos devidos e não se confunde com a estimativa do custo total

	(IST acumulado entre abr/2023 e maio/2022 de 2,93%)					(60 MESES)
	ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	
SD-WAN, Firewall UTM/NGFW, monitoramento, Zero Trust e MFA – Sede e unidades descentralizadas do Coren-SP	R$ 863.297,52	R$ 888.592,13	R$ 914.627,87	R$ 941.426,46	R$ 969.010,25	**R$ 4.576.954,23**

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

12.1. Da Descrição da Solução como um Todo

12.1.1. A Solução de TIC a ser contratada corresponde a Solução Integrada de Segurança de Rede, Autenticação e Conectividade.

12.1.2. A Contratada deverá fornecer todos os equipamentos, acessórios e programas necessários à instalação, operação e monitoração da Solução Contratada sem a cobrança de custos adicionais à Contratante. Ademais, os valores contratados deverão acobertar todos os custos relacionados à implantação da Solução, desde aqueles relacionados à disponibilização de infraestrutura, instalação e configuração de todos os hardwares, softwares, capacitação e serviços relacionados à Solução.

12.1.3. A Solução acima descrita, foi objeto de escolha pela Equipe de Planejamento da Contratação após consideração dos achados da análise comparativa de soluções/cenários viáveis, bem como dos valores dos custos totais de propriedade das respectivas soluções/cenários, com maior detalhamento no tópico de justificativa técnica da escolha da solução abaixo.

12.2. Das Hipóteses de Subcontratação

12.2.1. Vedada a subcontratação da parcela principal da Solução, considerada Solução Integrada de Segurança de Rede, Autenticação e Conectividade, a Administração permitirá, exclusivamente, a subcontratação de serviços e infraestrutura da ***'última milha'*** para viabilizar os serviços de links de acesso à internet das Subseções e Napes do Coren-SP, considerado que esse é um procedimento usual entre fornecedores de serviços de telecomunicações. No presente caso, todas as obrigações sobre a prestação dos serviços serão de responsabilidade da CONTRATADA, de forma que questões relativas a suporte, chamados, atualizações, questões administrativas, etc, serão tratadas somente entre a CONTRATANTE e a CONTRATADA, não devendo haver envolvimento da empresa subcontratada nessas interações.

12.2.2. Não será permitida a subcontratação da última milha para o link do tipo 2, destinado à Sede do Coren-SP, devendo a Contratada fornecer o link e o serviço de Anti-DDoS sem a participação de terceiros.

12.3. Da Apresentação e Aceitação da Proposta Comercial

12.3.1. A Proposta Comercial apresentada deverá informar detalhadamente o fabricante e os modelos de hardwares que serão empregados, bem como todos os detalhes de sua solução de conectividade à internet e demais itens de serviços componentes do objeto de contratação, informando protocolos, meios de transmissão e equipamentos a serem utilizados na implantação da Solução, podendo a Contratante solicitar informações adicionais.

---

da contratação estabelecida no subitem 13.1, uma vez que a aplicação de índice inflacionário ocorre por meio de apostilamento ao instrumento contratual.

12.3.2. A aprovação da Proposta Comercial estará sujeita à avaliação do atendimento dos requisitos e especificações técnicas estabelecidas pelo Coren-SP.

13. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

13.1. O custo anual estimado para a contratação do grupo único é R$ 863.297,57 (oitocentos e sessenta e três mil, duzentos e noventa e sete reais e cinquenta e sete centavos), chegando ao valor total estimado de R$ 4.316.486,60 (quatro milhões, trezentos e dezesseis mil, quatrocentos e oitenta e sete reais e sessenta centavos), conforme Apenso I e resumo da tabela abaixo:

GRUPO ÚNICO								
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**CATSER**	**UNIDADE DE MEDIDA**	**QTDE**	**VALOR UNITÁRIO ESTIMADO**	**VALOR MENSAL ESTIMADO**	**VALOR ANUAL ESTIMADO**	**VALOR TOTAL ESTIMADO (60 MESES)**
1	Link Tipo 1 - Link de comunicação de dados com largura de banda de 100 (cem) Mbps	26484	Serviço (mensal)	18	R$ 886,55	R$ 15.957,90	R$ 191.494,80	R$ 957.474,00
2	Link Tipo 2 - Link de comunicação de dados com largura de banda de 300 (trezentos) Mbps *com serviço de Anti-DDoS*	26484	Serviço (mensal)	2	R$ 2.386,67	R$ 4.773,34	R$ 57.280,08	R$ 286.400,40
3	Serviço de SD-WAN/Firewall - Tipo 1	26069	Serviço (mensal)	2	R$ 4.400,00	R$ 8.800,00	R$ 105.600,00	R$ 528.000,00
4	Serviço de SD-WAN/Firewall - Tipo 2	26069	Serviço (mensal)	18	R$ 633,79	R$ 11.408,22	R$ 136.898,64	R$ 684.493,20
5	Solução para conexão com MFA e proteção de usuários remotos	26077	Subscrição (mensal)	600	R$ 51,67	R$ 31.002,00	R$ 372.024,00	R$ 1.860.120,00
VALORES TOTAIS ESTIMADOS - GRUPO ÚNICO (ITENS 1 a 5)							**R$ 863.297,52**	**R$ 4.316.487,60**

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

14.1. Da Justificativa Técnica da Escolha da Solução Como um Todo e do Parcelamento da Solução Decorrente de Aspectos Técnicos

14.1.1. O cenário de contratação previsto neste ETP contempla a contratação de serviços de empresa especializada para fornecimento de Solução de SD-WAN com equipamentos concentradores do tipo UTM/NGFW para Segurança na Sede e nas unidades descentralizadas do Coren-SP, com MFA, Zero Trust, com monitoramento 24x7, treinamento, garantia e suporte.

14.1.2. Tal divisão, conforme explicações deste ETP, objetiva garantia de conectividade e segurança da rede corporativa do Coren-SP por meio de conexão principal e redundante à rede mundial de computadores na Sede, bem como instalação de componentes que possibilitem contratação futura de redundância nas unidades descentralizadas, conforme demanda futura, afastando riscos relacionados à segurança da informação e, por meio da conexão redundante, garantia de conectividade das unidades descentralizadas do Coren-SP, na eventualidade de queda de conexão da rede principal, acompanhando as boas práticas de TI e conferindo continuidade do funcionamento das atividades finalísticas e administrativas das unidades. A contratação de fornecedores diferentes para disponibilização de serviços de acesso principal e redundante para a Sede, objetiva a disponibilização de canais distintos para conexão à internet, de forma que a EPC, tendo identificado a demanda e partindo da premissa que os serviços de conexão redundante serão recursos utilizados secundariamente, previu tecnologia de link dedicado de acesso à internet, serviço de maior robustez e indicado aos clientes corporativos.

14.1.3. Ademais, conforme justificativas já prestadas neste ETP, a indicação de contratação pelo período de 60 (sessenta meses), possibilidade aberta pelo art. 106, *caput* da Lei nº 14.133/2021 para

a contratação de serviços de natureza continuada, mostra-se especialmente desejável para solução de altíssima criticidade para o funcionamento da instituição, afastando riscos relacionados a processos de transição contratual e, especialmente, relacionados à complexidade dos processos de implementação de soluções que, ainda que sejam comuns do ponto de vista de oferta, se mostram complexas do ponto de vista administrativo e técnico, tendo em vista que envolvem a instalação de infraestrutura específica entre unidades, preveem disponibilização de equipamentos, configuração e realização de testes de implantação, parametrização dos aspectos de segurança da Solução, capacitação da equipe de TI do Coren-SP dentre outros.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

15.1. Da Justificativa Técnica da Escolha da Solução Como um Todo e do Parcelamento da Solução

15.1.1. A contratação, com vigência contratual inicial sugerida para 60 (sessenta) meses, se tratando da parcela que carrega maior complexidade dentro do cenário proposto, além de possuir justificativas técnicas para vigência inicial superior a doze meses, cf. achados deste ETP, foi objeto de redução proporcional de custos, quando comparada a contratação firmada para 12 (doze) e 60 (sessenta) meses em pesquisa de preços realizada junto a fornecedores, correspondendo, logo, ao requisito exigido pelo inciso I do art. 106 da NLLC para a formalização de contratações plurianuais. Tem-se que, na contratação de serviços que envolvam a disponibilização de equipamentos e de infraestrutura específica por parte das contratadas, contratações em períodos superiores permitem diluição dos custos de implantação e também permitem melhores condições negociais, em função da expectativa de recebimentos por um período maior.

16. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

16.1. Em respeito a diversas leis que imputam responsabilidade na administração pública de realizar esforços para a obtenção de um ambiente de TI seguro, indicamos como essencial a contratação das soluções do referido objeto (Firewalls UTM/NGFW, MFA, Zero Trust e SD-WAN).

16.2. Como parte da missão de manter a segurança das informações, serviços e dados do Coren-SP, reassumida na Política de Segurança da Informação e Comunicações, é essencial que sejam implementadas soluções tecnológicas que busquem prezar pela Confidencialidade, Disponibilidade e Integridade dos serviços prestados à população.

16.3. Soluções de Infraestrutura e Segurança como SD-WAN, UTM/NGFW, Zero Trust e MFA hoje em dia são essenciais para a manutenção de um ambiente seguro e resiliente, capaz de responder a ameaças diversas em constante crescimento e aprimoramento na internet.

17. PROVIDÊNCIAS A SEREM ADOTADAS

17.1. As providências identificadas pela Equipe de Planejamento da Contratação, especialmente relacionadas à transição da Solução atualmente em operação para o ambiente proposto no presente ETP, estão detalhadas nos requisitos de capacitação e tópico 8.5 deste documento.

18. DECLARAÇÃO DE VIABILIDADE

18.1. Considerando os achados acima descritos, s.m.j., avalia-se como **viável** a contratação do objeto de estudos deste ETP.

APROVAÇÃO E ASSINATURA
Conforme os §§ 2º e 3º do Art. 11 da IN SGD/ME nº 94, de 23 de dezembro de 2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC[8]:

São Paulo, 15 de junho de 2023.

INTEGRANTE REQUISITANTE/ RESPONSÁVEL PELA ÁREA TÉCNICA (GTI)	INTEGRANTE TÉCNICO
Rafael Conceição da Silva Assinado de forma digital por Rafael Conceição da Silva Dados: 2023.06.15 16:05:15 -03'00' **Rafael Conceição da Silva** Gerente – GTI Matrícula 455	Regis de Oliveira Araujo Assinado de forma digital por Regis de Oliveira Araujo Dados: 2023.06.15 15:12:14 -03'00' **Régis de Oliveira Araújo** Analista de Segurança da Informação Matrícula 1044

INTEGRANTE DA ÁREA DE APOIO ADMINISTRATIVO
Henrique Pereira Soares Assinado de forma digital por Henrique Pereira Soares Dados: 2023.06.15 15:53:37 -03'00' **Henrique Pereira Soares** Assessor II – GAB/PRES Matrícula 975

[8] No caso do Coren-SP, a Autoridade Superior realiza a aprovação dos artefatos da contratação por meio de Despacho Circunstanciado encartado nos autos do Processo Administrativo de Contratação, cf. etapa 10 do Anexo I da Norma Interna Coren-SP/CG/NI/001/2013 – Versão 3.0.

CONSELHO FEDERAL DE ENFERMAGEM
CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

Anexos do documento ID 135450
(Listagem gerada, automaticamente, pelo sistema)

	Anexo ID	Tipo	Arquivo
1	99840	Anexos ETP	01_APENSO I - MAPAS COMPARATIVOS.pdf (Arquivo ID 552792)
2	99839	Anexos ETP	02_APENSO II - REQUISITOS TECNICOS DA SOLUCAO.pdf (Arquivo ID 552793)

APENSO I DO ETP - MAPAS COMPARATIVOS
PROCESSO ADMINISTRATIVO Nº 0142/2023

COMPARATIVO DE CUSTOS TOTAIS DE PROPRIEDADE - TCO (VIGÊNCIA INICIAL DE 12 MESES *X* 60 MESES)
Para verificação de vantajosidade, a EPC utilizou de propostas comerciais obtidas junto a fornecedores especializados (Algar Telecom, Bras Nuvem e Metodo Telecom)
Para ambos os cenários, desconsiderados custos inflacionários. Ainda, para ambos os casos, considerado o período total de vigência do contrato como de efetiva execução dos serviços.

VALORES TOTAIS ESTIMADOS - GRUPO ÚNICO (ITENS 1 a 5) - VIGÊNCIA INICIAL DE 12 (DOZE) MESES

ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	UNIDADE DE MEDIDA	QTDE	VALORES UNITÁRIOS OFERTADOS (fornecedores)			VALOR UNITÁRIO MEDIO (média simples)	VALOR MENSAL ESTIMADO	VALOR ANUAL ESTIMADO	VALOR TOTAL ESTIMADO (valor anual x 60 meses)
				ALGAR TELECOM	BRAS NUVEM	METODO TELECOM				
1	Link Tipo 1 - Link de comunicação de dados com largura de banda de 100 (cem) Mbps com serviço de Anti-DDoS	Serviço (mensal)	18	R$ 1.400,00	R$ 1.520,00	R$ 1.420,00	R$ 1.446,66	R$ 26.039,88	R$ 312.478,56	R$ 1.562.392,80
2	Link Tipo 2 - Link de comunicação de dados com largura de banda de 300 (trezentos) Mbps com serviço de Anti-DDoS	Serviço (mensal)	2	R$ 2.860,00	R$ 2.950,00	R$ 3.040,00	R$ 2.950,00	R$ 5.900,00	R$ 70.800,00	R$ 354.000,00
3	Serviço de SD-WAN/Firewall - Tipo 1	Serviço (mensal)	2	R$ 4.800,00	R$ 5.200,00	R$ 5.980,00	R$ 5.326,66	R$ 10.653,32	R$ 127.839,84	R$ 639.199,20
4	Serviço de SD-WAN/Firewall - Tipo 2	Serviço (mensal)	18	R$ 720,00	R$ 700,00	R$ 790,00	R$ 736,66	R$ 13.259,88	R$ 159.118,56	R$ 795.592,80
5	Solução para conexão com MFA e proteção de usuários remotos	Subscrição (mensal)	600	R$ 56,00	R$ 53,00	R$ 49,00	R$ 52,66	R$ 31.596,00	R$ 379.152,00	R$ 1.895.760,00
VALORES TOTAIS ESTIMADOS - GRUPO ÚNICO (ITENS 1 a 5) - VIGÊNCIA INICIAL DE 12 (DOZE) MESES									**R$ 1.049.388,96**	**R$ 5.246.944,80**

VALORES TOTAIS ESTIMADOS - GRUPO ÚNICO (ITENS 1 a 5) - VIGÊNCIA INICIAL DE 60 (SESSENTA) MESES

ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	UNIDADE DE MEDIDA	QTDE	VALORES UNITÁRIOS OFERTADOS (fornecedores)			VALOR UNITÁRIO MEDIO (média simples)	VALOR MENSAL ESTIMADO	VALOR ANUAL ESTIMADO	VALOR TOTAL ESTIMADO (60 MESES)
				ALGAR TELECOM	BRAS NUVEM	METODO TELECOM				
1	Link Tipo 1 - Link de comunicação de dados com largura de banda de 100 (cem) Mbps com serviço de Anti-DDoS	Serviço (mensal)	18	R$ 1.350,00	R$ 1.450,00	R$ 1.300,00	R$ 1.366,66	R$ 24.599,88	R$ 295.198,56	R$ 1.475.992,80
2	Link Tipo 2 - Link de comunicação de dados com largura de banda de 300 (trezentos) Mbps com serviço de Anti-DDoS	Serviço (mensal)	2	R$ 2.860,00	R$ 2.750,00	R$ 3.010,00	R$ 2.873,33	R$ 5.746,66	R$ 68.959,92	R$ 344.799,60
3	Serviço de SD-WAN/Firewall - Tipo 1	Serviço (mensal)	2	R$ 4.400,00	R$ 4.500,00	R$ 5.800,00	R$ 4.900,00	R$ 9.800,00	R$ 117.600,00	R$ 588.000,00
4	Serviço de SD-WAN/Firewall - Tipo 2	Serviço (mensal)	18	R$ 690,00	R$ 700,00	R$ 750,00	R$ 713,33	R$ 12.839,94	R$ 154.079,28	R$ 770.396,40
5	Solução para conexão com MFA e proteção de usuários remotos	Subscrição (mensal)	600	R$ 52,50	R$ 50,00	R$ 46,00	R$ 49,50	R$ 29.700,00	R$ 356.400,00	R$ 1.782.000,00
VALORES TOTAIS ESTIMADOS - GRUPO ÚNICO (ITENS 1 a 5) - VIGÊNCIA INICIAL DE 60 (SESSENTA) MESES									**R$ 992.237,76**	**R$ 4.961.188,80**

REDUÇÃO MEDIA APURADA EM CONTRATO DE DURAÇÃO INICIAL DE 60 (SESSENTA) MESES VERSUS CONTRATO DE 12 (DOZE MESES)	**5,45%**

PA Nº	142/2023	Solução SD-WAN e serviços de Firewall UTM/NGFW, monitoramento, Zero Trust e MFA	DATA DE VENCIMENTO DO MAPA	01/08/2023

GRUPO	ITEM	CÓDIGO CATMAT/CATSER	DESCRIÇÃO / ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA
ÚNICO	1	26484	Link Tipo 1 - Link de comunicação de dados com largura de banda de 100 (cem) Mbps	Serviço (mensal)	1

CÁLCULO DO VALOR REFERENCIAL		
PARÂMETRO	INICIAL	FINAL
VM	R$857,32	R$855,78
DESV PAD	564,30	546,78
CV	65,82%	63,89%
LIM SUP	R$1.421,62	R$1.402,56
LIM INF	R$293,02	R$309,00
MEDIANA	R$886,55	R$886,55

ID	PARÂMETROS	UASG - ÓRGÃO - LICITAÇÃO - ITEM - CNPJ DO FORNECEDOR / FORNECEDOR - CNPJ - CONTATO - SITE	DATA DA PESQUISA / DO ORÇAMENTO / DA LICITAÇÃO / DO CONTRATO	DATA DE VENCIMENTO DA REFERÊNCIA	PREÇO UNITÁRIO (R$)	UTILIZADO? SIM / NÃO	PREÇO UNITÁRIO REFERENCIAL	VALOR TOTAL ESTIMADO
a	II	UASG 926647 - CONSELHO REG.DOS REPRESENTANTES COMERCIAIS-PR - PE 02/2023 - CONNECTION - ADVISORY, OUTSOURCING AND SERVICES LTDA - CNPJ: 13.645.308/0001-36 ITEM 1 (item compatível, descrição do objeto exige link dedicado com 100 Mbps) - (data da homologação)	31/03/2023	30/03/2024	R$ 300,00	SIM	R$ 886,55	R$ 886,55
b	II	UASG 926089 - CONSELHO REGIONAL DE EDUCACAO FISICA 4A - SP - PE 22/2022 - B R A SERVICOS DE COMUNICACAO LTDA - CNPJ: 32.799.248/0001-50 - ITEM 2 (item compatível, descrição do objeto exige link dedicado com 100 Mbps) - (data da homologação)	30/12/2022	30/12/2023	R$ 270,83	NÃO		
c	II	UASG 389511 - SENAC - ADMINISTRACAO REGIONAL EM M. GERAIS - TELEFONICA BRASIL S.A - CNPJ/CPF: 02.558.157/0001-62 - ITEM 9 (item compatível, descrição do objeto exige link dedicado com 100 Mbps, selecionado valor para a cidade de Belo Horizonte) - (data da homologação)	22/08/2022	22/08/2023	R$ 473,10	SIM		
d	IV	ALGAR TELECOM S/A - CNPJ/CPF: 71.208.516/0001-74 - Fernando - (11) 99483-9607 - fernandoesc@algar.com.br (corresponde a valor da proposta para 60 meses) - (data da proposta)	02/02/2023	01/08/2023	R$ 1.350,00	SIM		
e	IV	BRAS NUVEM LTDA. - CNPJ: 43.600.363/0001-70 - Notile - notile@brasnuvem.com.br (corresponde ao valor da proposta para 60 meses) - (data da proposta)	26/05/2023	22/11/2023	R$ 1.450,00	NÃO		
f	IV	METODO TELECOMUNICACOES E COMERCIO LTDA - CNPJ: 65.295.172/0001-85 (corresponde ao valor da proposta para 60 meses) - (data da proposta)	18/05/2023	14/11/2023	R$ 1.300,00	SIM		

OBSERVAÇÕES E JUSTIFICATIVAS	

INSTRUÇÕES PARA AVALIAÇÃO DE PREÇOS	
	A) Calcular o valor médio (VM) inicial a partir dos orçamentos apresentados;
	B) Calcular o devio padrão (DESV PAD) inicial a partir dos mesmos orçamentos apresentados;
	C) Calcular o coeficiente de variação (CV) inicial pela divisão do DESV PAD INICIAL sobre o VM INICIAL;
	D) Se o CV INICIAL for menor ou igual a 25% (amostras homogêneas), considera-se como valor referencial o VM INICIAL;
	E) Caso contrário (amostras heterogêneas), calcular o limite superior (LIM SUP) inicial a partir da soma do VM INICIAL + DESV PAD INICIAL e o limite inferior (LIM INF) inicial a partir da subtração do VM INICIAL - DESV PAD INICIAL;
	F) Filtrar os orçamentos para que estejam dentro dos limites inferior e superior iniciais, colocando no campo utilizado como "SIM" aqueles que serão utilizados e como "NÃO" aqueles que serão descartados;
	G) Calcular o valor médio (VM) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	H) Calcular o devio padrão (DESV PAD) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	I) Calcular o coeficiente de variação (CV) final pela divisão do DESV PAD FINAL sobre o VM FINAL;
	J) Se o CV FINAL for menor ou igual a 25%, considera-se como valor referencial o VM FINAL;
	K) Caso contário, calcula-se a mediana final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO", que será utilizada como o valor referencial.
	L) Em todos os cenários deve haver no **mínimo 3 orçamentos** com o campo utilizado "SIM", devendo-se prospectar mais orçamentos ou **apresentar justificativa** no campo específico acima.

LOCAL, DATA DE PREENCHIMENTO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA PESQUISA	Regis de Oliveira Araujo, Analista de Segurança da Informação - GTI, Matrícula 1044
LOCAL, DATA DE REVISÃO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA REVISÃO	Henrique Pereira Soares, Assessor II - GAB/PRES, Matrícula 975

Rafael Conceição da Silva
Assinado de forma digital por Rafael Conceição da Silva
Dados: 2023.06.13 10:23:32 -03'00'

Regis de Oliveira Araujo
Assinado de forma digital por Regis de Oliveira Araujo
Dados: 2023.06.13 10:27:02 -03'00'

Henrique Pereira Soares
Assinado de forma digital por Henrique Pereira Soares
Dados: 2023.06.15 09:32:17 -03'00'

PA Nº	142/2023	Solução SD-WAN e serviços de Firewall UTM/NGFW, monitoramento, Zero Trust e MFA	DATA DE VENCIMENTO DO MAPA	26/04/2023

GRUPO	ITEM	CÓDIGO CATMAT/CATSER	DESCRIÇÃO / ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA
ÚNICO	2	26484	Link Tipo 3 - Link de comunicação de dados com largura de banda de 300 (trezentos) Mbps com serviço de Anti-DDoS	Serviço (mensal)	1

CÁLCULO DO VALOR REFERENCIAL		
PARÂMETRO	INICIAL	FINAL
VM	R$2.315,38	R$2.386,67
DESV PAD	645,90	455,75
CV	27,90%	19,10%
LIM SUP	R$2.961,28	R$2.842,42
LIM INF	R$1.669,48	R$1.930,92
MEDIANA	R$2.458,33	R$2.458,33

ID	PARÂMETROS	UASG - ÓRGÃO - LICITAÇÃO - ITEM - CNPJ DO FORNECEDOR / FORNECEDOR - CNPJ - CONTATO - SITE	DATA DA PESQUISA / DO ORÇAMENTO / DA LICITAÇÃO / DO CONTRATO	DATA DE VENCIMENTO DA REFERÊNCIA	PREÇO UNITÁRIO (R$)	UTILIZADO? SIM / NÃO	PREÇO UNITÁRIO REFERENCIAL	VALOR TOTAL ESTIMADO
a	II	UASG 925181 - CONSELHO REG QUIMICA 4A REGIAO (SP) - PE 26/2022 - CONNECTION - ADVISORY, OUTSOURCING AND SERVICES LTDA - CNPJ: 13.645.308/0001-36 - ITEM 2 (item compatível, descrição do objeto exige link dedicado com 300 Mbps + Anti-DDoS) - (data da homologação)	27/09/2022	27/09/2023	R$ 1.850,00	SIM	R$ 2.386,67	R$ 2.386,67
b	II	UASG 925466-TRIBUNAL DE CONTAS DO ESTADO DO PIAUI - PE 09/2022 - IT TECNOLOGIA E INFORMACAO LTDA - CNPJ/CPF: 00.608.881/0001-28 - ITEM 1 (item compatível, descrição do objeto exige link dedicado de 500 Mbps + Anti-Ddos - apesar da velocidade ser ligeiramente superior àquela exigida pelo Coren-SP, o item foi entendido como compatível para fins de pesquisa estimativa de preços, uma vez que se encontra, inclusive, abaixo de propostas comerciais obtidas para largura de banda inferior)	01/08/2022	01/08/2023	R$ 2.166,67	SIM		
c	II	UASG 80016 - TRIBUNAL REGIONAL DO TRABALHO DA 10A.REGIAO - R2 TELECOM COM. PROD. P / INF.LTDA - CNPJ: 72.639.628/0001-42 - ITEM 3 (item compatível, descrição do objeto exige link dedicado de 500 Mbps + Anti-Ddos - apesar da velocidade ser ligeiramente superior àquela exigida pelo Coren-SP, o item foi entendido como compatível para fins de pesquisa estimativa de preços, uma vez que se encontra, inclusive, abaixo de propostas comerciais obtidas para largura de banda inferior) - (valor unitário = R$ 1333,33 + aplicação do índice setorial IST, que foi de 0,17% para o mês de abril/2023, cf. informações obtidas no sítio da ANATEL).	26/04/2022	26/04/2023	R$ 1.335,60	NÃO	**R$ 2.386,67**	
d	IV	ALGAR TELECOM S/A - CNPJ/CPF: 71.208.516/0001-74 - Fernando - (11) 99483-9607 - fernandoesc@algar.com.br (corresponde a valor da proposta para 60 meses - Item link + Anti-DDoS) - (data da proposta)	02/02/2023	01/08/2023	R$ 2.780,00	SIM		
e	IV	BRAS NUVEM LTDA. - CNPJ: 43.600.363/0001-70 - Notile - notile@brasnuvem.com.br (corresponde a valor da proposta para 60 meses - Item link + Anti-DDoS) - (data da proposta)	26/05/2023	22/11/2023	R$ 2.750,00	SIM		
f	IV	METODO TELECOMUNICACOES E COMERCIO LTDA - CNPJ: 65.295.172/0001-85 (corresponde a valor da proposta para 60 meses - Item link + Anti-DDoS) - (data da proposta)	18/05/2023	14/11/2023	R$ 3.010,00	NÃO		

OBSERVAÇÕES E JUSTIFICATIVAS	

INSTRUÇÕES PARA AVALIAÇÃO DE PREÇOS	
	A) Calcular o valor médio (VM) inicial a partir dos orçamentos apresentados;
	B) Calcular o devio padrão (DESV PAD) inicial a partir dos mesmos orçamentos apresentados;
	C) Calcular o coeficiente de variação (CV) inicial pela divisão do DESV PAD INICIAL sobre o VM INICIAL;
	D) Se o CV INICIAL for menor ou igual a 25% (amostras homogêneas), considera-se como valor referencial o VM INICIAL;
	E) Caso contrário (amostras heterogêneas), calcular o limite superior (LIM SUP) inicial a partir da soma do VM INICIAL + DESV PAD INICIAL e o limite inferior (LIM INF) inicial a partir da subtração do VM INICIAL - DESV PAD INICIAL;
	F) Filtrar os orçamentos para que estejam dentro dos limites inferior e superior iniciais, colocando no campo utilizado como "SIM" aqueles que serão utilizados e como "NÃO" aqueles que serão descartados;
	G) Calcular o valor médio (VM) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	H) Calcular o devio padrão (DESV PAD) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	I) Calcular o coeficiente de variação (CV) final pela divisão do DESV PAD FINAL sobre o VM FINAL;
	J) Se o CV FINAL for menor ou igual a 25%, considera-se como valor referencial o VM FINAL;
	K) Caso contário, calcula-se a mediana final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO", que será utilizada como o valor referencial.
	L) Em todos os cenários deve haver no **mínimo 3 orçamentos** com o campo utilizado "SIM", devendo-se prospectar mais orçamentos ou **apresentar justificativa** no campo específico acima.

LOCAL, DATA DE PREENCHIMENTO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA PESQUISA	Regis de Oliveira Araujo, Analista de Segurança da Informação - GTI, Matrícula 1044
LOCAL, DATA DE REVISÃO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA REVISÃO	Henrique Pereira Soares, Assessor II - GAB/PRES, Matrícula 975

Rafael Conceição da Silva
Assinado de forma digital por Rafael Conceição da Silva
Dados: 2023.06.13 10:20:52 -03'00'

Regis de Oliveira Araujo
Assinado de forma digital por Regis de Oliveira Araujo
Dados: 2023.06.13 10:25:44 -03'00'

Henrique Pereira Soares
Assinado de forma digital por Henrique Pereira Soares
Dados: 2023.06.15 09:31:40 -03'00'

PA Nº	142/2023	Solução SD-WAN e serviços de Firewall UTM/NGFW, monitoramento, Zero Trust e MFA	DATA DE VENCIMENTO DO MAPA	01/08/2023

GRUPO	ITEM	CÓDIGO CATMAT/CATSER	DESCRIÇÃO / ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA
ÚNICO	3	26069	Serviço de SD-WAN/Firewall - Tipo 1	Serviço (mensal)	1

CÁLCULO DO VALOR REFERENCIAL		
PARÂMETRO	INICIAL	FINAL
VM	R$3.602,29	R$3.728,29
DESV PAD	1913,24	1251,03
CV	53,11%	33,56%
LIM SUP	R$5.515,53	R$4.979,32
LIM INF	R$1.689,05	R$2.477,26
MEDIANA	R$4.400,00	R$4.400,00

ID	PARÂMETROS	UASG - ÓRGÃO - LICITAÇÃO - ITEM - CNPJ DO FORNECEDOR / FORNECEDOR - CNPJ - CONTATO - SITE	DATA DA PESQUISA / DO ORÇAMENTO / DA LICITAÇÃO / DO CONTRATO	DATA DE VENCIMENTO DA REFERÊNCIA	PREÇO UNITÁRIO (R$)	UTILIZADO? SIM / NÃO	PREÇO UNITÁRIO REFERENCIAL	VALOR TOTAL ESTIMADO
a	IV	ALGAR TELECOM S/A - CNPJ/CPF: 71.208.516/0001-74 - Fernando - (11) 99483-9607 - fernandoesc@algar.com.br (corresponde a valor da proposta para 60 meses) - (data da proposta)	02/02/2023	01/08/2023	R$ 4.400,00	SIM	R$ 4.400,00	R$ 4.400,00
b	IV	BRAS NUVEM LTDA. - CNPJ: 43.600.363/0001-70 - Notile - notile@brasnuvem.com.br (corresponde ao valor da proposta para 60 meses) - (data da proposta)	26/05/2023	22/11/2023	R$ 4.500,00	SIM		
c	IV	METODO TELECOMUNICACOES E COMERCIO LTDA - CNPJ: 65.295.172/0001-85 (corresponde ao valor da proposta para 60 meses) - (data da proposta)	18/05/2023	14/11/2023	R$ 5.800,00	NÃO		
d	II	UASG 100001 - TRIBUNAL DE JUSTICA DO DISTRITO FEDERAL - PE 63/2022 - BRFIBRA TELECOMUNICACOES LTDA - CNPJ: 73.972.002/0001-16 - Item 1 (item com configurações compatíveis ao equipamento do tipo 1 descrito pelo Coren-SP)	20/04/2023	19/04/2024	R$ 2.284,88	SIM		
e	II	UASG 928680 - NAV BRASIL SERVIÇOS DE NAVEGACÃO AEREA S.A. - PE 02/2023 - OI SOLUCOES S/A - CNPJ: 09.719.875/0001-12 - SDWAN Tipo 1 (item com configurações compatíveis ao equipamento do tipo 1 descrito pelo Coren-SP)	08/02/2023	08/02/2024	R$ 1.026,58	NÃO		

OBSERVAÇÕES E JUSTIFICATIVAS	

INSTRUÇÕES PARA AVALIAÇÃO DE PREÇOS	
	A) Calcular o valor médio (VM) inicial a partir dos orçamentos apresentados;
	B) Calcular o devio padrão (DESV PAD) inicial a partir dos mesmos orçamentos apresentados;
	C) Calcular o coeficiente de variação (CV) inicial pela divisão do DESV PAD INICIAL sobre o VM INICIAL;
	D) Se o CV INICIAL for menor ou igual a 25% (amostras homogêneas), considera-se como valor referencial o VM INICIAL;
	E) Caso contrário (amostras heterogêneas), calcular o limite superior (LIM SUP) inicial a partir da soma do VM INICIAL + DESV PAD INICIAL e o limite inferior (LIM INF) inicial a partir da subtração do VM INICIAL - DESV PAD INICIAL;
	F) Filtrar os orçamentos para que estejam dentro dos limites inferior e superior iniciais, colocando no campo utilizado como "SIM" aqueles que serão utilizados e como "NÃO" aqueles que serão descartados;
	G) Calcular o valor médio (VM) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	H) Calcular o devio padrão (DESV PAD) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	I) Calcular o coeficiente de variação (CV) final pela divisão do DESV PAD FINAL sobre o VM FINAL;
	J) Se o CV FINAL for menor ou igual a 25%, considera-se como valor referencial o VM FINAL;
	K) Caso contário, calcula-se a mediana final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO", que será utilizada como o valor referencial.
	L) Em todos os cenários deve haver no **mínimo 3 orçamentos** com o campo utilizado "SIM", devendo-se prospectar mais orçamentos ou **apresentar justificativa** no campo específico acima.

LOCAL, DATA DE PREENCHIMENTO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA PESQUISA	Regis de Oliveira Araujo, Analista de Segurança da Informação - GTI, Matrícula 1044
LOCAL, DATA DE REVISÃO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA REVISÃO	Henrique Pereira Soares, Assessor II - GAB/PRES, Matrícula 975

Rafael Conceição da Silva
Assinado de forma digital por Rafael Conceição da Silva
Dados: 2023.06.13 10:21:07 -03'00'

Regis de Oliveira Araujo
Assinado de forma digital por Regis de Oliveira Araujo
Dados: 2023.06.13 10:28:12 -03'00'

Henrique Pereira Soares
Assinado de forma digital por Henrique Pereira Soares
Dados: 2023.06.15 09:31:52 -03'00'

PA Nº	142/2023	Solução SD-WAN e serviços de Firewall UTM/NGFW, monitoramento, Zero Trust e MFA	DATA DE VENCIMENTO DO MAPA	01/08/2023

GRUPO	ITEM	CÓDIGO CATMAT/CATSER	DESCRIÇÃO / ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA
ÚNICO	4	26069	Serviço de SD-WAN/Firewall - Tipo 2	Serviço (mensal)	1

CÁLCULO DO VALOR REFERENCIAL		
PARÂMETRO	INICIAL	FINAL
VM	R$633,79	N/A
DESV PAD	133,27	N/A
CV	21,03%	N/A
LIM SUP	R$767,06	N/A
LIM INF	R$500,52	N/A
MEDIANA	R$690,00	N/A

ID	PARÂMETROS	UASG - ÓRGÃO - LICITAÇÃO - ITEM - CNPJ DO FORNECEDOR / FORNECEDOR - CNPJ - CONTATO - SITE	DATA DA PESQUISA / DO ORÇAMENTO / DA LICITAÇÃO / DO CONTRATO	DATA DE VENCIMENTO DA REFERÊNCIA	PREÇO UNITÁRIO (R$)	UTILIZADO? SIM / NÃO	PREÇO UNITÁRIO REFERENCIAL	VALOR TOTAL ESTIMADO
a	IV	ALGAR TELECOM S/A - CNPJ/CPF: 71.208.516/0001-74 - Fernando - (11) 99483-9607 - fernandoesc@algar.com.br (corresponde a valor da proposta para 60 meses) - (data da proposta)	02/02/2023	01/08/2023	R$ 690,00	SIM	R$ 633,79	R$ 633,79
b	IV	BRAS NUVEM LTDA. - CNPJ: 43.600.363/0001-70 - Notile - notile@brasnuvem.com.br (corresponde ao valor da proposta para 60 meses) - (data da proposta)	26/05/2023	22/11/2023	R$ 700,00	SIM		
c	IV	METODO TELECOMUNICACOES E COMERCIO LTDA - CNPJ: 65.295.172/0001-85 (corresponde ao valor da proposta para 60 meses) - (data da proposta)	18/05/2023	14/11/2023	R$ 750,00	SIM		
d	II	UASG 100001 - TRIBUNAL DE JUSTICA DO DISTRITO FEDERAL - PE 63/2022 - BRFIBRA TELECOMUNICACOES LTDA - CNPJ: 73.972.002/0001-16 - Item 2 (item com configurações compatíveis ao equipamento do tipo 2 descrito pelo Coren-SP)	20/04/2023	19/04/2024	R$ 618,20	SIM		
e	II	UASG 928680 - NAV BRASIL SERVIÇOS DE NAVEGACÃO AEREA S.A. - PE 02/2023 - OI SOLUCOES S/A - CNPJ: 09.719.875/0001-12 - SDWAN Tipo 2 (item com configurações compatíveis ao equipamento do tipo 1 descrito pelo Coren-SP)	08/02/2023	08/02/2024	R$ 410,74	SIM		

OBSERVAÇÕES E JUSTIFICATIVAS	

INSTRUÇÕES PARA AVALIAÇÃO DE PREÇOS	
	A) Calcular o valor médio (VM) inicial a partir dos orçamentos apresentados;
	B) Calcular o devio padrão (DESV PAD) inicial a partir dos mesmos orçamentos apresentados;
	C) Calcular o coeficiente de variação (CV) inicial pela divisão do DESV PAD INICIAL sobre o VM INICIAL;
	D) Se o CV INICIAL for menor ou igual a 25% (amostras homogêneas), considera-se como valor referencial o VM INICIAL;
	E) Caso contrário (amostras heterogêneas), calcular o limite superior (LIM SUP) inicial a partir da soma do VM INICIAL + DESV PAD INICIAL e o limite inferior (LIM INF) inicial a partir da subtração do VM INICIAL - DESV PAD INICIAL;
	F) Filtrar os orçamentos para que estejam dentro dos limites inferior e superior iniciais, colocando no campo utilizado como "SIM" aqueles que serão utilizados e como "NÃO" aqueles que serão descartados;
	G) Calcular o valor médio (VM) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	H) Calcular o devio padrão (DESV PAD) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	I) Calcular o coeficiente de variação (CV) final pela divisão do DESV PAD FINAL sobre o VM FINAL;
	J) Se o CV FINAL for menor ou igual a 25%, considera-se como valor referencial o VM FINAL;
	K) Caso contário, calcula-se a mediana final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO", que será utilizada como o valor referencial.
	L) Em todos os cenários deve haver no **mínimo 3 orçamentos** com o campo utilizado "SIM", devendo-se prospectar mais orçamentos ou **apresentar justificativa** no campo específico acima.

LOCAL, DATA DE PREENCHIMENTO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA PESQUISA	Regis de Oliveira Araujo, Analista de Segurança da Informação - GTI, Matrícula 1044
LOCAL, DATA DE REVISÃO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA REVISÃO	Henrique Pereira Soares, Assessor II - GAB/PRES, Matrícula 975

Rafael Conceição da Silva
Assinado de forma digital por Rafael Conceição da Silva
Dados: 2023.06.13 10:21:23 -03'00'

Regis de Oliveira Araujo
Assinado de forma digital por Regis de Oliveira Araujo
Dados: 2023.06.13 10:29:10 -03'00'

Henrique Pereira Soares
Assinado de forma digital por Henrique Pereira Soares
Dados: 2023.06.15 09:32:05 -03'00'

PA Nº	142/2023	Solução SD-WAN e serviços de Firewall UTM/NGFW, monitoramento, Zero Trust e MFA	DATA DE VENCIMENTO DO MAPA	01/08/2023

GRUPO	ITEM	CÓDIGO CATMAT/CATSER	DESCRIÇÃO / ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA
ÚNICO	5	26077	Solução para conexão com MFA e proteção de usuários remotos	Subscrição (mensal)	1

CÁLCULO DO VALOR REFERENCIAL		
PARÂMETRO	INICIAL	FINAL
VM	R$51,67	N/A
DESV PAD	5,13	N/A
CV	9,93%	N/A
LIM SUP	R$56,80	N/A
LIM INF	R$46,54	N/A
MEDIANA	R$53,00	N/A

ID	PARÂMETROS	UASG - ÓRGÃO - LICITAÇÃO - ITEM - CNPJ DO FORNECEDOR / FORNECEDOR - CNPJ - CONTATO - SITE	DATA DA PESQUISA / DO ORÇAMENTO / DA LICITAÇÃO / DO CONTRATO	DATA DE VENCIMENTO DA REFERÊNCIA	PREÇO UNITÁRIO (R$)	UTILIZADO? SIM / NÃO	PREÇO UNITÁRIO REFERENCIAL	VALOR TOTAL ESTIMADO
a	IV	ALGAR TELECOM S/A - CNPJ/CPF: 71.208.516/0001-74 - Fernando - (11) 99483-9607 - fernandoesc@algar.com.br (corresponde a valor da proposta para 60 meses) - (data da proposta)	02/02/2023	01/08/2023	R$ 56,00	SIM	R$ 51,67	R$ 51,67
b	IV	BRAS NUVEM LTDA. - CNPJ: 43.600.363/0001-70 - Notile - notile@brasnuvem.com.br (corresponde ao valor da proposta para 60 meses) - (data da proposta)	26/05/2023	22/11/2023	R$ 53,00	SIM		
c	IV	METODO TELECOMUNICACOES E COMERCIO LTDA - CNPJ: 65.295.172/0001-85 (corresponde ao valor da proposta para 60 meses) - (data da proposta)	18/05/2023	14/11/2023	R$ 46,00	SIM		

OBSERVAÇÕES E JUSTIFICATIVAS	

INSTRUÇÕES PARA AVALIAÇÃO DE PREÇOS	
	A) Calcular o valor médio (VM) inicial a partir dos orçamentos apresentados;
	B) Calcular o devio padrão (DESV PAD) inicial a partir dos mesmos orçamentos apresentados;
	C) Calcular o coeficiente de variação (CV) inicial pela divisão do DESV PAD INICIAL sobre o VM INICIAL;
	D) Se o CV INICIAL for menor ou igual a 25% (amostras homogêneas), considera-se como valor referencial o VM INICIAL;
	E) Caso contrário (amostras heterogêneas), calcular o limite superior (LIM SUP) inicial a partir da soma do VM INICIAL + DESV PAD INICIAL e o limite inferior (LIM INF) inicial a partir da subtração do VM INICIAL - DESV PAD INICIAL;
	F) Filtrar os orçamentos para que estejam dentro dos limites inferior e superior iniciais, colocando no campo utilizado como "SIM" aqueles que serão utilizados e como "NÃO" aqueles que serão descartados;
	G) Calcular o valor médio (VM) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	H) Calcular o devio padrão (DESV PAD) final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO";
	I) Calcular o coeficiente de variação (CV) final pela divisão do DESV PAD FINAL sobre o VM FINAL;
	J) Se o CV FINAL for menor ou igual a 25%, considera-se como valor referencial o VM FINAL;
	K) Caso contário, calcula-se a mediana final a partir dos orçamentos em que o campo utilizado constar "SIM", descartando aqueles que estiverem como "NÃO", que será utilizada como o valor referencial.
	L) Em todos os cenários deve haver no **mínimo 3 orçamentos** com o campo utilizado "SIM", devendo-se prospectar mais orçamentos ou **apresentar justificativa** no campo específico acima.

LOCAL, DATA DE PREENCHIMENTO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA PESQUISA	Regis de Oliveira Araujo, Analista de Segurança da Informação - GTI, Matrícula 1044
LOCAL, DATA DE REVISÃO DO MAPA	São Paulo, 12/06/2023	IDENTIFICAÇÃO DO AGENTE RESPONSÁVEL PELA REVISÃO	Henrique Pereira Soares, Assessor II - GAB/PRES, Matrícula 975

Rafael Conceição da Silva
Assinado de forma digital por Rafael Conceição da Silva
Dados: 2023.06.13 10:20:35 -03'00'

Regis de Oliveira Araujo
Assinado de forma digital por Regis de Oliveira Araujo
Dados: 2023.06.13 10:29:51 -03'00'

Henrique Pereira Soares
Assinado de forma digital por Henrique Pereira Soares
Dados: 2023.06.15 09:32:30 -03'00'

CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

APENSO II DO ETP – REQUISITOS TÉCNICOS DA SOLUÇÃO
PROCESSO ADMINISTRATIVO Nº 142/2023

O seguinte caderno de especificações técnicas define os requisitos técnicos mínimos da Solução que deverão ser observados pela Contratada para atendimento das necessidades do Coren-SP relacionadas à contratação de serviços de **Solução Integrada de Segurança de Rede, Autenticação e Conectividade.**

Os requisitos técnicos se encontram divididos em seções, organizadas em títulos tecnicamente classificados, correspondendo aos itens de serviço do grupo único que formam a Solução como um todo.

1. DO GERENCIAMENTO CENTRALIZADO DA SOLUÇÃO E RELATORIA/CENTRALIZAÇÃO DE LOGS

1.1. DO GERENCIAMENTO CENTRALIZADO

1.1.1. O equipamento destinado ao gerenciamento centralizado deverá ser um virtual appliance hospedado em ambiente da CONTRATADA, disponibilizado na modalidade de nuvem ou em ambiente da contratante em virtualização HYPERVISOR, desde que seja do mesmo fabricante dos equipamentos de SD-WAN e NGFW para fins de interoperabilidade.

1.1.2. Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

1.1.2.1. Possuir compatibilidade com o Microsoft Hyper-V 2022 e superior;

1.1.2.2. Não deverá limitar o número de múltiplas vCPUs;

1.1.2.3. Não deverá definir limites para a expansão da memória RAM;

1.1.2.4. Deverá gerenciar, no mínimo, 30 (trinta) unidades (NGFW ou Sistemas Virtuais) dos equipamentos SD-WAN/NGFW de forma simultânea;

1.1.2.5. Como parte da visibilidade dos dispositivos gerenciados centralmente, a Solução deverá ter visibilidade do status do link, desempenho do aplicativo, utilização da largura de banda e conformidade com o SLA objetivo;

1.1.2.6. Possuir a capacidade de automatizar fluxos de trabalho e configurações para dispositivos gerenciados em uma única console;

1.1.2.7. Possuir recurso de Multi-tenancy para separar os dados de gerenciamento da infraestrutura lógica ou geograficamente e permitir a implantação do zero touch para o rápido provisionamento em massa;

1.1.2.8. Executar backups de configuração automáticos em até 5 (cinco) nós, contendo atualizações de todos os dispositivos gerenciados;

1.1.2.9. Possuir a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console e exibir sua localização geográfica em um mapa;

1.1.2.10. Permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança.

1.1.3. A ferramenta de Gerenciamento da Solução deverá:

1.1.3.1. Suportar acesso via SSH, cliente, WEB (HTTPS), SNMP V2 e API aberta;

1.1.3.2. Permitir acesso concorrente de administradores;

1.1.3.3. Possuir interface baseada em linha de comando para administração da solução de gerência;

1.1.3.4. Possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.1.3.5. Possuir funcionalidade de bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

1.1.3.6. Possibilitar a definição de perfis de acesso à console com permissões granulares, tais como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

1.1.3.7. Gerar alertas automáticos via E-mail;

1.1.3.8. Gerar alertas automáticos via SNMP;

1.1.3.9. Gerar alertas automáticos via Syslog;

1.1.3.10. Suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora incluindo recorrência no agendamento;

1.1.3.11. Permitir ao Administrador transferir os backups para um servidor SCP;

1.1.3.12. Permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;

1.1.3.13. Permitir aos administradores se autenticarem nos servidores de gerência através de bases externas TACACS, LDAP e RADIUS;

1.1.3.14. Permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);

1.1.3.15. Suportar sincronização do relógio interno via protocolo NTP;

1.1.3.16. Registrar as ações efetuadas por quaisquer usuários;

1.1.3.17. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

1.1.3.18. Permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

1.1.3.19. Permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

1.1.3.20. Permitir criar administradores que tenham acesso à todas as instancias de virtualização;

1.1.3.21. Garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

1.1.3.22. Possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema de prevenção a intrusão (IPS – Intrusion Prevention System), antivírus, filtro de URL;

1.1.3.23. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

1.1.3.24. Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

1.1.3.25. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

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

1.1.3.27. Permitir a criação de regras com data de expiração;

1.1.3.28. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (ou, alternativamente, garantir que esta exigência seja plenamente atendida por meio diverso);

1.1.3.29. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

1.1.3.30. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência, assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

1.1.3.31. Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;

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

1.2. DA RELATORIA E CENTRALIZAÇÃO DE LOGS

1.2.1. O equipamento deve ser um virtual appliance hospedado em ambiente da CONTRATADA, disponibilizado na modalidade de nuvem, ou implantando dentro do ambiente da contratante em virtualização HYPERVISOR, desde que, seja do mesmo fabricante da solução de SD-WAN e NGFW para fins de interoperabilidade.

1.2.2. Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

1.2.2.1. Possuir compatibilidade com o Microsoft Hyper-v 2022 e superior;

1.2.2.2. Gerenciar, no mínimo, 30 (trinta) unidades (NGFW ou Sistemas Virtuais) dos equipamentos da solução de NGFW de forma simultânea;

1.2.2.3. Suportar a coleta de até 5GB de logs por dia;

1.2.2.4. Suportar armazenamento de até 30 dias de regras habilitadas de segurança (UTM) ou de acordo com o ambiente de storage da Contratante;

1.2.2.5. Não deverá limitar o número de múltiplas vCPUs;

1.2.2.6. Não deverá haver limites para a expansão da memória RAM;

1.2.2.7. O licenciamento do produto com todas as funcionalidades relatadas deve ser válido durante todo o período do fornecimento do serviço;

1.2.2.8. Suportar o acesso via SSH, WEB (HTTPS) e SNMP V2 para gerenciamento da Solução;

1.2.2.9. Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando na console de gerenciamento;

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

1.2.2.11. Possuir suporte para SNMP versão 2 e 3 com disponibilidade de MIB;

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

1.2.2.13. Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

1.2.2.14. Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH;

1.2.2.15. Suportar a autenticação de usuários de acesso à plataforma via: LDAP, Radius e TACACS+;

1.2.2.16. Garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego;

1.2.2.17. Possuir mecanismo para que logs antigos sejam removidos automaticamente, após estarem consolidados na solução de guarda e análise de logs e relatoria;

1.2.2.18. Permitir a extração de relatórios;

1.2.2.19. Garantir a exportação dos logs;

1.2.2.20. Possuir relatórios pré-definidos;

1.2.2.21. Permitir a geração de relatórios de logs de tráfego de dados;

1.2.2.22. Possuir a capacidade de personalização de gráficos como barra, linha, tabela e pizza, para inserção aos relatórios;

1.2.2.23. Possuir mecanismo para exibir de forma detalhada informações complementares nos relatórios em tempo real;

1.2.2.24. Possibilitar o download dos arquivos de logs recebidos;

1.2.2.25. Possibilitar o envio de maneira automática de relatórios por e-mail;

1.2.2.26. Permitir a customização de quaisquer relatórios fornecidos pela Solução, exclusivamente a critério da Contratante, adaptando-o às suas necessidades;

1.2.2.27. Possuir a capacidade de definir filtros nos relatórios;

1.2.2.28. Ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;

1.2.2.29. Garantir a capacidade de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios;

1.2.2.30. Dispor de relatórios contemplando informações do ambiente, dos eventos de segurança e incidentes, das ameaças, do uso da navegação web, de IPS, da utilização da rede, entre outros;

1.2.2.31. Disponibilizar uma avaliação consolidada das ameaças cibernéticas;

1.2.2.32. Dispor de painel gráfico para análise das ameaças detectadas englobando controle de aplicação, IPS, filtro web e antivírus, demonstrando ainda os principais destinos, principais ameaças, principais incidentes de vírus, entre outros.

2. DA SOLUÇÃO DE FIREWALL (UTM/NGFW)

2.1. DOS REQUISITOS GERAIS

2.1.1. A Solução deverá consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD- WAN, não sendo permitido appliances virtuais ou solução open source (produto montado). Ademais, não serão aceitas soluções baseadas em PCs de uso geral e sim soluções baseadas em appliances desenvolvidos especificamente para a função de firewall.

2.1.1.1. Por funcionalidades de NGFW se entendam o reconhecimento de aplicações, a prevenção de ameaças, a identificação de usuários e o controle granular de permissões;

2.1.1.2. Por funcionalidades de SD-WAN se entendam o roteamento inteligente, o uso do melhor link por aplicação, a abstração do tráfego em relação aos circuitos físicos e o controle do tráfego por aplicação.

2.1.2. A Solução de comunicação de dados entre as unidades utilizará equipamentos com a tecnologia SD-WAN, **todos da mesma marca e compatíveis entre si, de forma a garantir a compatibilidade e interoperabilidade da Solução**;

2.1.3. A Gestão do Firewall, naquilo que se refere à aplicação de regras, bloqueios, políticas, entre outras funcionalidades, deverão ser de forma híbrida entre a Contratada e Contratante;

2.1.4. A Contratada deverá fornecer acesso aos equipamentos (senhas de acesso), para a contratante para fazer a gestão híbrida dos equipamentos;

2.1.5. Considerando a criticidade e o período previsto de contratação, os componentes da Solução deverão ser novos, sem uso, e entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios necessários às suas instalações;

2.1.6. Todos os roteadores e equipamentos necessários para a conexão entre os pontos deverão ser fornecidos, instalados, configurados, mantidos, gerenciados e operados pela Contratada;

2.1.7. Em caso de atualização de sistema que acrescentem novas funcionalidades aos equipamentos elas devem funcionar sem a necessidade de aquisição de nova licença;

2.1.8. Caso o fabricante remova o produto de linha, o mesmo deve substituir o produto entregue pela nova geração com capacidade e funcionalidades igual ou superior ao removido da linha de produção;

2.1.9. Os equipamentos deverão possuir garantia do fabricante de hardware e software durante a vigência do contrato;

2.1.10. Os equipamentos deverão possuir licenciamento perpetuado para as funcionalidades;

2.1.11. Deve possuir licenciamento durante a vigência do contrato para as subscrições de filtro de conteúdo, Antivírus, Controle de aplicação, IPS e outras que façam parte do produto e da oferta.

2.1.12. As funcionalidades de segurança e SD-WAN que compõem a Solução poderão funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos especificados neste caderno

e acompanhem os mesmos termos de garantia, atualizações e manutenção, suporte e gerenciamento centralizado;

2.1.13. A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7;

2.1.14. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 2U cada;

2.1.15. Deverão ser disponibilizados cabos de alimentação e, caso necessários, kits do tipo trilho para adaptação;

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

2.1.17. Os equipamentos disponibilizados deverão possuir suporte a 256 VLAN Tags 802.1Q;

2.1.18. Os equipamentos disponibilizados deverão possuir suporte a agregação de links 802.3ad LACP.

2.2. DOS REQUISITOS DOS DISPOSITIVOS DE PROTEÇÃO DE REDE

2.2.1. Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

2.2.1.1. Possuir suporte a VLANs;

2.2.1.2. Possuir suporte a roteamento multicast (PIM-SM);

2.2.1.3. Suportar BGPv4/BGP4+, OSPFv2/v3, RIP e roteamento estático;

2.2.1.4. Possuir suporte a DHCP Relay;

2.2.1.5. Possuir suporte a DHCP Server;

2.2.1.6. Suportar sub-interfaces ethernet lógicas;

2.2.1.7. Suportar NAT dinâmico (Many-to-Many);

2.2.1.8. Suportar NAT estático (1-to-1);

2.2.1.9. Suportar NAT estático bidirecional 1-to-1;

2.2.1.10. Suportar Tradução de porta (PAT);

2.2.1.11. Suportar NAT de Origem;

2.2.1.12. Suportar NAT de Destino;

2.2.1.13. Suportar NAT de Origem e NAT de Destino simultaneamente;

2.2.1.14. Implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

2.2.1.15. Suportar NAT46, NAT64;

2.2.1.16. Implementar o protocolo ECMP;

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

2.2.1.18. Enviar log para sistemas de monitoração externos;

2.2.1.19. Possuir a funcionalidade de enviar logs para os sistemas de monitoração externos via protocolo SSL;

2.2.1.20. Deverá possuir proteção anti-spoofing;

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

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

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

2.2.1.24. Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

2.3. DA CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DOS DISPOSITIVOS

2.3.1. A configuração em alta disponibilidade dos dispositivos ofertados na Solução deverá sincronizar:

2.3.1.1. Sessões;

2.3.1.2. Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;

2.3.1.3. Associações de Segurança das VPNs;

2.3.1.4. Tabelas FIB;

2.3.2. A Configuração em alta disponibilidade da Solução contratada deverá possibilitar, ainda:

2.3.2.1. Possibilitar monitoração de falha de link no modo de alta disponibilidade (HA);

2.3.2.2. Possuir suporte a criação de sistemas virtuais no mesmo appliance;

2.3.2.3. 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;

2.3.2.4. Controlar, inspecionar e realizar descriptografia de SSL para tráfego de Saída (Outbound);

2.4. DAS FUNCIONALIDADES DE IPS:

2.4.1. Os seguintes requisitos relacionados às funcionalidades de IPs deverão ser atendidos pela Solução ofertada:

2.4.1.1. Permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

2.4.1.2. Possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

2.4.1.3. Possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

2.4.1.4. Possuir capacidade de remontagem de pacotes para identificação de ataques;

2.4.1.5. Utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas;

2.4.1.6. Realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego.

2.4.1.7. Possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego;

2.4.1.8. Possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

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

2.4.1.10. Implementar, pelo menos, os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo;

2.4.1.11. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento;

2.4.1.12. Permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos;

2.4.1.13. Possibilitar a criação de políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos;

2.4.1.14. Possibilitar a criação de políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, entre outros;

2.4.1.15. Possibilitar escanear e bloquear conexões a servidores de botnet;

2.4.1.16. Dispor de opção para bloquear URLs maliciosas mediante base de dados local;

2.4.1.17. Possibilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS;

2.4.1.18. Suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS;

2.4.1.19. Suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros;

2.4.1.20. Possibilitar o filtro de assinaturas com base no identificador CVE;

2.4.1.21. Possibilitar a criação de uma assinatura de IPS utilizando o identificador CVE, bem como um “wildcard” do CVE para abranger mais de um identificador. As assinaturas deverão dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável;

2.4.1.22. Incluir proteção contra ataques de negação de serviços;

2.4.1.23. Registrar na console de monitoramento 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.

2.5. DAS FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

2.5.1. Os seguintes requisitos relacionados às funcionalidades de proteção contra ameaças avançadas deverão ser atendidos pela Solução ofertada:

2.5.1.1. Possuir funções de antivírus e anti-spyware;

2.5.1.2. Possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;

2.5.1.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros);

2.5.1.4. Dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a análise baseada em assinaturas;

2.5.1.5. Permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;

2.5.1.6. Permitir o bloqueio de download de arquivos por tamanho;

2.5.1.7. Realizar a mitigação de ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

2.5.1.8. Dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros.

2.5.2. Dentre as análises efetuadas, a Solução deverá suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back.

2.5.2.1. A solução de sandbox deverá ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque;

2.5.2.2. A solução de sandbox deverá ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente;

2.5.3. A Solução deverá analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deverá, ainda, disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento.

2.6. DAS FUNCIONALIDADES DE FILTROS WEB E DE CONTEÚDO

2.6.1. Os seguintes requisitos relacionados às funcionalidades de filtro WEB e de conteúdo deverão ser atendidos pela Solução ofertada:

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

2.6.1.2. Possibilitar a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

2.6.1.3. 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;

2.6.1.4. Permitir SSO por meio da identificação pela base do Active Directory, de forma que os usuários não precisem 'logar' novamente na rede para navegar pelo firewall;

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

2.6.1.6. Possuir a função de exclusão de URLs do bloqueio;

2.6.1.7. Permitir a customização de página de bloqueio;

2.6.1.8. Dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário;

2.6.1.9. Possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego;

2.6.1.10. Possuir funcionalidade que permita o bloqueio de tráfego HTTP POST (método utilizado para envio de informação a um determinado website);

2.6.1.11. Fltrar e remover Java Applets, ActiveX e cookies do tráfego web inspecionado;

2.6.2. Possuir, em sua base de dados, uma lista de bloqueio contendo URLs de certificados maliciosos;

2.6.3. Filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo;

2.6.4. Permitir, além do Web Proxy explícito, suporte ao proxy Web transparente.

2.7. DO FIREWALL TIPO 1 - EQUIPAMENTO UTM/NGFW:

2.7.1. Deverão ser disponibilizados 2 (dois) equipamentos principais, destinados à unidade Sede do Coren-SP, com instalação definida para cada segmento de rede (front-end e back-end).

2.7.2. Desempenho mínimo dos equipamentos (throughput mínimo) conforme Datasheet do fabricante:

2.7.2.1. UTM/NGFW (Full com todas as funcionalidades de segurança): 3.5Gbps;

2.7.2.2. IPS: 5Gbps;

2.7.2.3. VPN SSL: 2 Gbps;

2.7.3. Quantidade Mínima de Interfaces (fora as interfaces que eventualmente sejam necessárias para o funcionamento das conexões SD-WAN com as Subseções/NAPEs):

2.7.3.1. Oito (8) interfaces de 1gb (RJ45);

2.7.3.2. Quatro (4) interfaces de 10gb (fibra SFP(+) ou Oito (8) interfaces de 1gb (fibra SFP(+));

2.7.3.3. As interfaces tratadas nos subitens acima devem ser entregues junto com os equipamentos e estarem prontas para uso na entrega do objeto, incluindo eventuais licenciamentos adicionais que sejam necessários para isso.

2.7.4. Máximo de usuários simultâneos autenticados no firewall: Sem limite de licença ou de software;

2.7.5. Máximos de sessões simultâneas no firewall: mínimo de 3 (três) milhões;

2.7.6. Os equipamentos disponibilizados deverão incluir licenças para SSL VPN (ou VPN especifica do fabricante através de cliente próprio) para, pelo menos, 500 (quinhentos) usuários simultâneos no firewall externo (onde as conexões VPN serão feitas);

2.7.7. A VPN client-to-site deverá possuir, pelo menos, uma possibilidade de configuração rápida e utilização intuitiva por parte dos usuários como um cliente próprio de VPN ou cliente do fabricante, que agregue outras funções de segurança dessa contratação, como o Zero Trust por exemplo;

2.7.8. Os equipamentos ofertados deverão dispor de suporte completo ao SD-WAN ofertado e integração com os demais firewalls ofertados na Solução contratada pelo Coren-SP;

2.7.9. Ademais, os seguintes requisitos técnicos relacionados às funcionalidades dos dispositivos de proteção do tipo 1 deverão ser atendidos pela Solução ofertada:

2.7.9.1. Possibilitar a definição de quais máquinas, tipos, SOs, poderão acessar a VPN SSL, seja utilizando funcionalidade da VPN ou do Zero Trust;

2.7.9.2. Possibilitar a conferência de se a máquina é do Coren-SP ou não. Para isso poderá utilizar diversas técnicas presentes no mercado, como utilização de certificação digital nas máquinas autorizadas, ou outros;

2.7.9.3. Possibilitar o bloqueio temporário de IPs nas hipóteses de 'match' em determinada regra de negação, na tentativa de acesso a portas em blacklist e nas ações de portscan, IPscan, DoS ou DDoS;

2.7.9.4. Possuir funcionalidades de reconhecimento de aplicações, de prevenção de ameaças e de identificação de usuários;

2.7.9.5. Possuir otimização para a análise de conteúdo de aplicações;

2.7.9.6. Possuir suporte a Policy based routing ou policy based forwarding;

2.7.9.7. Suportar sub-interfaces ethernet logicas;

2.7.9.8. Suportar SD-WAN de forma nativa;

2.7.9.9. 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;

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

2.7.9.11. Possuir suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

2.7.9.12. Dispor de funcionalidade de Inspeção SSL sem limitação de licenciamento caso a solução ofertada possua licenciamento, deve ser fornecido em sua capacidade máxima;

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

2.7.9.14. Suportar, na console de administração, ao menos, o idioma inglês;

2.7.9.15. Realizar controles de políticas por porta e protocolo;

2.7.9.16. Realizar controles de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

2.7.9.17. Realizar controle de políticas por usuários do AD, grupos de usuários do AD, IPs, redes e zonas de segurança;

2.7.9.18. Suportar a inspeção UTM/NGFW (Application Control e Webfiltering, no mínimo) diretamente às políticas de segurança;

2.7.9.19. Suportar o padrão de indústria 'syslog' protocol para armazenamento;

2.7.9.20. Suportar integração com Solução de SIEM multi fabricante;

2.7.9.21. Suportar a integração nativa com soluções de sandboxing;

2.7.9.22. Possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.7.9.23. Reconhecer e permitir configurações de ações de permissão ou bloqueio de pelo menos 100 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, VPN, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

2.7.9.24. 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 utilização da rede Tor;

2.7.9.25. De-criptografar pacotes, para tráfego criptografado SSL, a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

2.7.9.26. Atualizar a base de assinaturas de aplicações automaticamente;

2.7.9.27. Permitir, o fabricante, a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

2.7.9.28. Possibilitar a diferenciação de tráfegos de Instant Messaging (Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

2.7.9.29. Possibilitar a diferenciação de aplicações Proxies (Psiphon, Freegate etc.) possuindo granularidade de controle/políticas para os mesmos;

2.7.9.30. Possibilitar a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

2.7.9.31. Possibilitar a criação de grupos estáticos de aplicações baseados em características das aplicações como categoria da aplicação;

2.7.9.32. Possuir, para proteção do ambiente contra ataques módulo de IPS, Antivírus e Anti-Spam integrados no próprio appliance de firewall;

2.7.9.33. Possuir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus);

2.7.9.34. Possibilitar bloqueios por reputação da origem;

2.7.9.35. Garantir a operação das funcionalidades de IPS e Antivírus em caráter permanente, podendo ser utilizadas por tempo indeterminado dentro do período do contrato e respectivas licenças;

2.7.9.36. Sincronizar as assinaturas de IPS e Antivírus quando implementado em alta disponibilidade;

2.7.9.37. Permitir o bloqueio de exploração de vulnerabilidades;

2.7.9.38. Realizar proteção contra ataques de negação de serviços;

2.7.9.39. Possuir os seguintes mecanismos de inspeção de IPS:

a) Análise para detecção de anomalias de protocolo;

b) IP Defragmentation;

c) Remontagem de pacotes de TCP;

d) Bloqueio de pacotes malformados;

2.7.9.40. Ser imune e capaz de impedir ataques básico, tais como, Syn flood, ICMP flood, UDP flood etc.;

2.7.9.41. Detectar e bloquear a origem de portscans;

2.7.9.42. Bloquear ataques efetuados por worms conhecidos;

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

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

2.7.9.45. Identificar e bloquear comunicação com botnets;

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

2.7.9.47. Permitir identificar, na ocorrência de eventos, o país de onde partiu a ameaça;

2.7.9.48. Incluir proteção contra vírus em conteúdo HTML e Javascript e softwares espiões (spyware) e worms;

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

2.7.9.50. 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 ou explícito;

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

2.7.9.52. Possuir, pelo menos, 60 categorias ou subcategorias de URLs;

2.7.9.53. Possuir a função de exclusão de URLs ou categorias do bloqueio;

2.7.9.54. Possibilitar a implementação de controle de navegação por usuário e grupo do AD sem necessidade de instalação de programas clientes em estações de trabalho dos usuários;

2.7.9.55. Possibilitar a implementação de controle de navegação por usuário e grupo do AD para usuários de serviços de terminal remoto em servidores RDS Windows Server;

2.7.9.56. Possuir funcionalidade de DLP para os principais tipos de conteúdo e/ou para criação de conteúdos customizáveis;

2.7.9.57. Possuir suporte a Link Aggregation;

2.7.9.58. Possuir suporte a multiwan load balance;

2.7.9.59. Possuir suporte a failover de WAN;

2.7.9.60. Possuir suporte total a IPv6;

2.7.9.61. Possibilitar o fechamento VPN site-to-site com serviços como Azure e AWS;

2.7.9.62. Permitir a escolha do Administrador referente a qual link de saída de internet será usado dependendo da regra em questão;

2.7.9.63. Dispor de funcionalidade de filtragem e visualização de logs em tempo real e históricos;

2.7.9.64. Permitir controle de consumo de banda pelo menos por regra de firewall, origem ou aplicação;

2.7.9.65. Permitir a customização de página de bloqueio de internet/navegação;

2.7.9.66. Suportar web proxy transparente com inspeção de SSL, sem necessidade de configurações na máquina dos usuários, apenas através de roteamento de gateway padrão;

2.7.9.67. Possibilitar a 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 RADIUS;

2.7.9.68. Possuir integração com o 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. A funcionalidade em questão não deverá possuir limites licenciados de usuários ou qualquer tipo de restrição de uso, a exemplo de utilização de sistemas virtuais, segmentos de rede, etc;

2.7.9.69. Possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory de forma que, caso seja necessário instalar cliente nas estações, esse deverá ser o mesmo utilizado no ZTNA e outras funcionalidades de segurança;

2.7.9.70. Possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.7.9.71. Permitir que se faça o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, se expanda um portal de autenticação residente no firewall (Captive Portal), nas hipóteses de falha do SSO;

2.7.9.72. 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;

2.7.9.73. Proporcionar, com a finalidade de controlar aplicações de camada 7 e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda (a exemplo de Youtube, Ustream etc.), permitir ou negar esse tipo de aplicação, devendo, ademais, 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 streaming de vídeo;

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

2.7.9.75. Permitir a criação de filtros para arquivos e dados pré-definidos em HTTP e SMTP;

2.7.9.76. Realizar identificação de arquivos por extensão e tipo (primeiros bits);

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

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

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

2.7.9.80. Permitir a utilização das funcionalidades de VPN Site-to-Site e Client-To-Site;

2.7.9.81. Suportar VPN em IPv4 e IPv6;

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

2.7.9.83. Permitir que todo o tráfego dos usuários remotos de VPN (SSL ou IPSEc) seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

2.7.9.84. Permitir criar políticas de firewall, de controle de aplicações, IPS, Antivírus e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

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

2.7.9.86. Permitir bloqueios de APT;

2.7.9.87. Proporcionar compatibilidade com do agente de VPN SSL ou IPSEC client-to-site com: Windows 10 (32 e 64 bits) ou superior, Windows 11 (32 e 64 bits) ou superior Linux Ubuntu 21.04 LTS ou superior e Mac OS v10.15 (Catalina) ou superior, Android 12 ou superior e iOS 15 ou superior;

2.7.9.88. Suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

2.7.9.89. Permitir criação de regras de navegação e firewall apenas na gerência centralizada ou na console dos firewalls principais, com replicação automática para os

firewalls remotos instalados nas Subseções e NAPEs, aplicando o controle SD-WAN para uso de internet pelo link local das unidades descentralizadas, utilizando a banda local, sem comprometer o link da unidade Sede, mas ainda assim aplicando as políticas de navegação e segurança definidas;

2.7.9.90. Bloquear o acesso a conteúdo indevido ao utilizar a pesquisa de buscadores web, tais como Google, Yahoo etc., independentemente de a opção Safe Search estar habilitada no navegador do usuário.

2.8. DO FIREWALL TIPO 2 – EQUIPAMENTO UTM/NGFW

2.8.1. Deverá ser disponibilizado um (1) equipamento UTM/NGFW para cada unidade descentralizadas em funcionamento do Coren-SP, para controle de SD-WAN e políticas de segurança das Subseções e NAPEs do Coren-SP relacionadas no Termo de Referência.

2.8.2. Os equipamentos disponibilizados deverão receber e aplicar as políticas geradas em console centralizada ou na gerência do próprio firewall da unidade Sede (Firewall Tipo 1).

2.8.3. Os seguintes requisitos técnicos relacionados às funcionalidades dos dispositivos de proteção do tipo 2 deverão ser atendidos pela Solução ofertada:

2.8.3.1. Throughput de, no mínimo, 4 Gbps com a funcionalidade de firewall habilitada;

2.8.3.2. Suporte a, no mínimo, 650.000 de conexões simultâneas (TCP);

2.8.3.3. Suporte a, no mínimo, 30.000 novas conexões por segundo (TCP);

2.8.3.4. Throughput de no mínimo 2,5 Gbps de VPN IPSec, com pacotes de, no mínimo, 512 bytes;

2.8.3.5. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos;

2.8.3.6. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de clientes VPN IPSEC simultâneos;

2.8.3.7. Suportar, no mínimo, 900 Mbps de throughput de IPS;

2.8.3.8. Suportar, no mínimo, 700 Mbps de throughput de controle de aplicação;

2.8.3.9. Suportar, no mínimo, 300 Mbps de throughput de Inspeção SSL;

2.8.3.10. Throughput de, no mínimo, 490 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware;

2.8.3.11. Possuir, ao menos, 4 interfaces RJ45;

2.8.3.12. Possuir porta USB compatível com modem 3G/4G, permitindo ainda que este link WAN seja utilizado nas regras de SD- WAN;

2.8.3.13. Possuir fonte de alimentação com fonte DC de 100–240V AC, 50–60hz.

As funcionalidades a seguir devem seguir funcionando, mesmo após o vencimento do contrato de suporte e licenciamento: SD-WAN, controle de aplicação e stateful firewall;

3. DA CONEXÃO E PROTEÇÃO DE USUÁRIOS REMOTOS (MFA E ZERO TRUST)

3.1. A presente seção contempla requisitos relacionados à VPN (já especificada na seção 2 deste documento, que trata dos firewalls), à Autenticação Multifatorial (MFA) e ao Zero Trust (ZTNA).

3.2. DA AUTENTICAÇÃO MULTIFATORIAL (MFA)

3.2.1. As funcionalidades da solução de autenticação multifatorial ofertada não deverão excluir ou impactar em termos de desempenho àquelas das demais parcelas da Solução a ser contratada pelo Coren-SP, mas sim, complementá-las, em termos de funcionalidades.

3.2.2. Considerando a projeção de demanda da Contratante, a Solução ofertada ao Coren-SP deverá possibilitar a utilização da autenticação multifatorial para, pelo menos, 750 (setecentos e cinquenta) usuários simultaneamente[1].

3.2.3. A Solução poderá corresponder a um appliance dedicado instalado na infraestrutura da Contratante ou hospedada em Nuvem, desde que atenda aos requisitos definidos neste caderno de especificações técnicas.

3.2.4. A MFA, para o ambiente do Coren-SP, se prestará à autenticação de duplo fator para os usuários VPN cliente-to-site, do Firewall UTM/NGFW e para outras aplicações Web via protocolos de integração.

3.2.5. Ademais, os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

3.2.5.1. Possuir capacidade de integração com aplicações Web desenvolvidas internamente no Coren-SP. Ademais, a Solução deverá possuir funcionalidade que permita a criação de um Hub MFA ou Portal/Gateway para implementar a autenticação MFA à frente de aplicações que não possuam suporte às integrações MFA da Solução ofertada (no presente caso, a Contratada poderá utilizar de outra aplicação do mesmo fabricante da Solução MFA ofertada para atendimento do requisito);

3.2.5.2. Possuir capacidade de configuração de MFA em um portal SAML;

3.2.5.3. Para o provisionamento das autorizações de acesso dos usuários na interface de administração da Solução, deverá ser utilizada, ao menos, a integração com o serviço de diretório AD, correspondendo à associação de usuários aos grupos de usuários (perfis), sendo obtida do serviço de diretório AD;

3.2.5.4. Suportar múltiplos domínios de Microsoft Active Directory;

3.2.5.5. Para utilização pelos usuários para autenticação em múltiplos dispositivos, a Solução deverá suportar, no mínimo, os sistemas operacionais: Windows, Android e iOS, utilizando aplicativo próprio ou aplicativo de autenticação de mercado gratuito, como o Authy, o MS Authenticator ou o Google Authenticator;

3.2.5.6. Disponibilizar portal de autoatendimento ao usuário para provisionamento e/ou desprovisionamento do seu dispositivo. O portal em questão deverá possuir, no mínimo, autenticação por meio de usuário e senha de diretório (AD/LDAP) e através de integração SAML;

[1] Importa destacar que, a princípio, o Coren-SP estima a contratação inicial de aproximadamente 300 (trezentas) licenças, de forma que as demais licenças serão incorporadas ao objeto de faturamento à medida do incremento das demandas do Coren-SP, durante a vigência do instrumento contratual, com ativações solicitadas por meio do envio de Ordens de Serviço (OS) à Contratada.

3.2.5.7. Possibilitar que o usuário não consiga remover a exigência do uso do fator adicional da solução;

3.2.5.8. Registrar todas as atividades realizadas, tanto de usuários quanto de administradores, gerando log com, no mínimo, as informações de data e hora, usuário, endereço de origem e informações completas das operações;

3.2.5.9. Registras as falhas e exceções em log com informações suficientes para identificação da falha, com no mínimo as informações de data e hora, usuário e endereço de origem;

3.2.5.10. Manter o histórico de todas as informações geradas pela solução e que sofreram inclusões, alterações e exclusões por parte dos usuários da solução;

3.2.5.11. Permitir a consulta e exportação das trilhas de auditoria, logs e históricos;

3.2.5.12. Disponibilizar geração de relatório de utilização do múltiplo fator de autenticação;

3.2.5.13. Não limitar a quantidade de aplicações a ser utilizada;

3.2.5.14. Dispor de mecanismos de contingência para que, caso ocorra a interrupção da conexão de acesso à internet ou na ocorrência de indisponibilidade do serviço, os usuários possam continuar se autenticando no ambiente;

3.2.5.15. Dispor de capacidade de integração com o Security Assertion Markup Language – SAML;

3.2.5.16. Dispor de capacidade de integração com o Active Directory Federation Services – ADFS;

3.2.5.17. Dispor de capacidade de integração com Remote Authentication Dial-In User Service – RADIUS;

3.2.5.18. Disponibilizar, pelo menos, os seguintes fatores de autenticação:

a) Push Notification (notificação enviada para uma aplicação instalada no dispositivo do usuário);

b) Software Token – OTP (One Time Password);

c) OTP enviado por Short Message Service – SMS;

3.2.5.19. Permitir a criação de políticas para definir quais usuários terão obrigatoriedade de utilização de múltiplo fator de autenticação;

3.2.5.20. Permitir a criação de políticas baseadas no comportamento do usuário (MFA Adaptativo) para permitir o acesso ou não ao ambiente, pelo menos para os seguintes itens (pode ser utilizada outra solução do mesmo fabricante (com licença inclusa) para atendimento desse requisito):

a) Redes autorizadas;

b) Por geolocalização;

c) Dispositivo.

3.2.5.21. Possuir compatibilidade com os navegadores Microsoft Edge, Mozilla Firefox e Google Chrome;

3.2.5.22. Permitir acesso aos administradores da Solução via interface Web, não exigindo a instalação de complementos, plug-ins ou extensões para seu pleno funcionamento;

3.2.5.23. Permitir a criação de diferentes perfis de usuários, com diferentes níveis de autorização, permissões e visões, garantindo que as permissões de acesso sejam gerenciadas a partir da interface da solução;

3.2.5.24. Permitir que somente usuários administradores sejam capazes de criar, alterar ou remover usuários e suas permissões associadas conforme perfis.

3.3. DO MODELO DE SEGURANÇA DE CONFIANÇA ZERO (ZERO TRUST NETWORK ACCESS - ZTNA)

3.3.1. As funcionalidades da solução de segurança de confiança zero ofertada não deverão excluir ou impactar em termos de desempenho àquelas das demais parcelas da Solução a ser contratada pelo Coren-SP, mas sim, complementá-las, em termos de funcionalidades.

3.3.2. Considerando a projeção de demanda da Contratante, a Solução ofertada ao Coren-SP deverá possibilitar a utilização do ZTNA para, pelo menos, 750 (setecentos e cinquenta) usuários simultaneamente[2].

3.3.3. O ZTNA poderá ser parte integrante da Solução de firewall, ser um appliance dedicado instalado na infraestrutura da Contratante ou uma solução em Nuvem, desde que atenda aos requisitos definidos neste caderno de especificações técnicas.

3.3.4. O gateway das conexões do agente cliente deverá ser o próprio firewall ofertado ou recurso de nuvem;

3.3.5. O ZTNA, para o ambiente do Coren-SP, se prestará a garantir que apenas máquinas autorizadas e seguras acessem a rede do Coren-SP, seja na infraestrutura local, seja por cliente VPN client-to-site, podendo o ZTNA utilizar o mesmo cliente de VPN, ou outros.

3.3.6. Ademais, os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

3.3.6.1. Possuir possibilidade de integração com aplicações web desenvolvidas internamente no Coren-SP, executando checagens no cliente para autorizar ou não o acesso a aplicação;

3.3.6.2. Possuir funcionalidade de Proxy ZTNA para publicação de um serviço pra internet sem necessidade de passar pela VPN, fazendo todas as checagens de segurança do cliente através de atribuição de tags (rótulos);

3.3.6.3. Possuir cliente a ser instalado nos endpoints para atribuição de tags de segurança, minimamente compatível com Windows 10 ou superior, Linux, últimas versões do MacOS, iOS e Android;

3.3.6.4. Possibilitar que os clientes endpoint sejam instalados remotamente pela gerência;

[2] Importa destacar que, a princípio, o Coren-SP estima a contratação inicial de aproximadamente 300 (trezentas) licenças, de forma que as demais licenças serão incorporadas ao objeto de faturamento à medida do incremento das demandas do Coren-SP, durante a vigência do instrumento contratual, com ativações solicitadas por meio do envio de Ordens de Serviço (OS) à Contratada.

3.3.6.5. Possibilitar a atribuição automática pelo programa cliente de tags de segurança, a partir de regras definidas na gerência. As tags em questão poderão ser manipuladas na gerência centralizada, bem como poderão ser criadas políticas para tratamento dos endpoints com base nas tags recebidas;

3.3.6.6. Permitir ou negar acesso a uma determinada rede/recurso/serviço com base na tag atribuída;

3.3.6.7. Realizar envio das tags aos clientes em tempo real, sem a necessidade de estarem na rede da empresa ou na VPN, através, apenas, de conexão com a internet;

3.3.6.8. Realizar a atribuição de tags com base, minimamente, nos seguintes requisitos:

a) Se está logado no domínio AD da empresa;

b) Se a máquina está remota ou local na empresa (pelo menos por range IP);

c) Se a máquina possui Antivírus ativado e qual versão;

d) Se a máquina executa algum programa em blacklist;

e) Se a máquina possui vulnerabilidades (sistema e aplicativos não atualizados e vulneráveis);

f) Se a versão do sistema operacional é aceitável ou não;

g) Se a máquina possui um determinado certificado;

h) Se a máquina possui uma chave de registro especifica;

i) Se a máquina possui um arquivo específico;

j) Se faz parte de um grupo específico do AD.

4. DOS SERVIÇOS CONECTIVIDADE (SD-WAN E LINKS)

4.1. A presente seção contempla requisitos relacionados aos serviços de conectividade, relacionados à tecnologia SD-WAN e aos serviços de links dedicados de comunicação de dados para acesso à internet destinado à unidade Sede e unidades descentralizadas do Coren-SP.

4.2. DA TECNOLOGIA SD-WAN

4.2.1. Entende-se como tecnologia SD-WAN a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos.

4.2.2. As funcionalidades da tecnologia SD-WAN deverão ser contempladas no UTM/NGFW;

4.2.3. Os seguintes requisitos técnicos deverão ser atendidos pela Solução ofertada:

4.2.3.1. Prover recursos de roteamento inteligente, definindo, mediante regras preestabelecidas, o melhor caminho a ser tomado para uma aplicação;

4.2.3.2. Possibilitar o monitoramento e identificação de falhas mediante a associação de health check, permitindo testes de resposta por ping, http e tcp/udp echo;

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

4.2.3.4. Permitir a definição do roteamento para cada aplicação;

4.2.3.5. Permitir padrões de escolha do link, 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;

4.2.3.6. Possibilitar a definição do link de saída para uma aplicação específica;

4.2.3.7. Implementar balanceamento de link por hash do IP de origem e de destino;

4.2.3.8. Implementar balanceamento de link por peso. Na opção em questão, deverá ser possível definir o percentual de tráfego que será escoado por cada um dos links. Ademais, deverá suportar o balanceamento de, no mínimo, dois links;

4.2.3.9. Implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

4.2.3.10. Possuir suporte a Policy based routing ou policy based forwarding;

4.2.3.11. Suportar roteamento estático e dinâmico (OSPF, BGP);

4.2.3.12. Possibilitar a agregação de túneis IPsec;

4.2.3.13. Possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

4.2.3.14. 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;

4.2.3.15. 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, a Solução deverá, 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 a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

a) por endereço de origem;

b) por endereço de destino;

c) por usuário e grupo;

d) por aplicações;

e) por porta.

4.2.3.16. Possibilitar, pelo QoS, a definição de tráfego com banda garantida, a exemplo de banda mínima disponível para aplicações de negócio;

4.2.3.17. Possibilitar, pelo QoS, a definição de tráfego com banda máxima, a exemplo de banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc.;

4.2.3.18. Possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

4.2.3.19. Possibilitar, pelo QoS, a definição de fila de prioridade;

4.2.3.20. Possibilitar a definição de banda máxima e garantida por aplicação, devendo, também, suportar essas definições com base em categorias de URL, IPs de origem e destino, logins e portas;

4.2.3.21. Possuir a capacidade de agendar intervalos de tempo durante os quais as políticas de shaping/QoS poderão ser alteradas, a exemplo de regra de controle de banda mais permissivas durante o horário de almoço;

4.2.3.22. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que se enquadrarem na regra ou por IP, a exemplo de 10 Mbps de banda garantida por IP ou para todos os IPs que se enquadrem na regra;

4.2.3.23. Possibilitar a definição de bandas distintas para download e upload;

4.2.3.24. Prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

4.2.3.25. Suportar IPv6;

4.2.3.26. Possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

4.2.3.27. Possibilitar o bloqueio de acesso a aplicações;

4.2.3.28. Suportar NAT dinâmico bem como NAT de saída;

4.2.3.29. Suportar balanceamento de tráfego por sessão e pacote;

4.2.3.30. Implementar balanceamento de link por custo configurado do link;

4.2.3.31. Suportar o balanceamento de, no mínimo, 5 links;

4.2.3.32. Suportar o balanceamento de links de interfaces físicas, sub- interfaces lógicas de VLAN e túneis IPSec;

4.2.3.33. Suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links;

4.2.3.34. Gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;

4.2.3.35. Suportar Zero-Touch Provisioning;

4.2.3.36. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de latência, jitter e perda de pacotes;

4.2.3.37. Configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Tais valores serão utilizados pela solução para decidir qual link será utilizado;

4.2.3.38. Permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;

4.2.3.39. A checagem de estado de saúde deverá suportar teste com Ping, HTTP e DNS;

4.2.3.40. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e protocolo;

4.2.3.41. Suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD- WAN;

4.2.3.42. Suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;

4.2.3.43. Possibilitar a utilização do balanceamento round robin na agregação de duas ou mais IPSEC VPNs determinando o peso para cada VPN;

4.2.3.44. Possibilitar especificar o número mínimo de interfaces ativas em uma regra de SD-WAN para que esta regra seja válida;

4.2.4. Nas localidades em onde houver disponibilidade de banda larga, a Solução deverá ser capaz de promover redundância entre os links de internet dedicada e internet banda larga de forma que na eventualidade de indisponibilidade do link principal (internet dedicada) o sistema possa automaticamente utilizar o link alternativo (internet banda larga) para manter as conexões sempre ativas.

4.3. DOS LINKS DE ACESSO DEDICADO À INTERNET

4.3.1. Trata-se da prestação de serviços de acesso à Internet por meio de links dedicados com largura de banda de 100 (cem) e 300 (trezentos) Mbps e Firewall;

4.3.2. Os serviços fornecidos deverão ter as características técnicas conforme especificações constantes neste instrumento, atendendo, no mínimo, às seguintes características:

4.3.2.1. Banda simétrica;

4.3.2.2. Suporte a pacotes IP com MTU mínimo de 1.500 Bytes;

4.3.2.3. Taxas de transmissão e quantidade de links e IP's por link de acordo com a seguinte tabela:

UNIDADE/LOCALIDADE[3]	QTDE LINKS ATIVOS	LARGURA DE BANDA (Mbps)	QTD IPv4 POR LINK
Unidade Sede - São Paulo/SP	2	300	16
Nape Alto Tietê (Mogi das Cruzes/SP) – MOGI	1	100	1
Subseção Araçatuba – ARA	1	100	1
Subseção Botucatu – BOT	1	100	1
Subseção Campinas – CAM	1	100	1
Subseção Guarulhos – GRU	1	100	1
Subseção Itapetininga – ITA	1	100	1
Subseção Marília – MAR	1	100	1
Subseção Osasco – OSA	1	100	1
Subseção Presidente Prudente – PP	1	100	1
Nape Registro – REG (AGUARDA ABERTURA)[4]	1	100	1

[3] Relação de endereços das unidades disponível em: https://portal.coren-sp.gov.br/fale-conosco/enderecos/.

UNIDADE/LOCALIDADE[3]	QTDE LINKS ATIVOS	LARGURA DE BANDA (Mbps)	QTD IPv4 POR LINK
Subseção Ribeirão Preto – RP	1	100	1
Nape Santa Cecília (São Paulo/SP) – SC	1	100	1
Nape Santo Amaro (São Paulo/SP) – AMR	1	100	1
Subseção Santo André – AND	1	100	1
Subseção Santos – SAN	1	100	1
Subseção São José do Rio Preto – SJRP	1	100	1
Subseção São José dos Campos – SJC	1	100	1
Nape Sorocaba – SOR	1	100	1

4.3.2.4. Endereços IPv6 deverão ser fornecidos de acordo com o padrão para usuário de internet, ou seja, ranges de máscara 48 ou 56 para cada link;

4.3.2.5. Taxas de transferência de dados em modo simétrico (recepção = transmissão) de, pelo menos 100 ou 300 Mbps, a depender da localidade, em um único enlace ou em múltiplos enlaces agrupados, entregues no mesmo roteador. Caso os serviços sejam ofertados por meio de mais de um enlace, estes deverão estar configurados para balanceamento automático de carga e a conexão com a rede do CONTRATANTE deverá ser feita por meio de uma única porta Ethernet;

4.3.2.6. 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;

4.3.2.7. A largura da banda contratada deverá estar 100% disponível para tráfego de dados entre o firewall instalado no CONTRATANTE e o roteador de serviços durante todo o período de seu funcionamento;

4.3.2.8. 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;

4.3.2.9. O meio físico do transporte de dados deverá ser por meio de redes de fibra óptica, a serem entregues e instaladas nos locais indicados pela Contratante, ficando a Contratada responsável integralmente pelos custos de infraestrutura e de instalação das conexões;

4.3.2.10. A comunicação de dados não poderá ser feita por meios aéreos de comunicação (satélite ou rede sem fio) na última milha, devendo ser estas realizadas por meio terrestre;

4.3.2.11. Caberá à CONTRATADA prover todo o cabeamento externo necessário à disponibilização do serviço a ser fornecido até o primeiro ponto de acesso dentro das instalações do Coren-SP;

[4] Unidade com abertura planejada, porém sem data de inauguração definida. Assim sendo, a Administração virá a solicitar a contratação dos serviços em questão a partir da definição da data de inauguração definida, a ocorrer durante a vigência contratual, formalizando a ativação dos serviços por meio do envio de Ordem de Serviço (OS) à Contratada.

4.3.2.12. Especificamente, em relação aos links dedicados de 300 Mbps, destinados à unidade Sede do Coren-SP:

4.3.2.12.1. Os caminhos físicos utilizados em cada um dos links deverão estar separados entre si. Nesta situação, tanto os equipamentos (modem, roteador, etc.) quanto os meios físicos da rede de acesso deverão ser redundantes e tolerantes a falhas, isto é, cada link dedicado deverá possuir uma estrutura própria, devendo chegar ao endereço da unidade Sede do Coren-SP por caminhos distintos.

4.3.2.12.2. Em virtude da segurança e disponibilidade dos sistemas, acessos e serviços publicados e tendo em vista que o serviço operará em contingência ativa, os dois links contratados deverão operar em esquema de tolerância a falhas ativo/ativo, usando técnica de cluster com protocolo VRRP, de modo a garantir a alta disponibilidade do serviço de acesso à Internet. Cada equipamento deverá "ser responsável" por um dos dois ranges de IP contratados e estes equipamentos deverão ser configurados de forma que, no caso de falha em um deles, o que permanecer disponível passe a responder pelas duas faixas de IPs, (tanto pela sua própria quanto pela daquele que está indisponível). Essa configuração deverá persistir pelo tempo que o equipamento/link indisponível permanecer neste estado, devendo retornar assim que o mesmo voltar à atividade.

4.3.2.13. A comunicação dos links não poderá sofrer limitações de velocidade ou restrições à quantidade de dados trafegados, tais como traffic shaping;

4.3.2.14. Os serviços não poderão sofrer qualquer espécie de redução quanto ao tempo de conexão ou ao volume de dados trafegado (conexão ilimitada);

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

4.3.2.16. Todos os serviços de implantação dos links de acesso à internet deverão ser entregues em pleno funcionamento, nas condições técnicas estabelecidas pela Contratante. A Contratada deverá, para tanto, disponibilizar todos os equipamentos necessários à prestação dos serviços, tais como modens, roteadores e outros necessários, sem ônus para a Contratante;

4.3.2.17. Na execução dos serviços, a Contratada ficará responsável pelas seguintes ações, sem custos adicionais à Contratante:

a) Serviços de gerência proativa da rede;

b) Serviços de configuração dos equipamentos fornecidos;

c) Serviços de integração e testes de cada link fornecido;

d) Serviços de manutenção dos links, com substituição em caso de defeito nos equipamentos, garantindo a continuidade do serviço;

e) Serviços esporádicos relativos ao remanejamento de links, juntamente com os seus equipamentos;

4.3.2.18. A CONTRATADA se responsabilizará por eventuais adaptações nas instalações físicas nas dependências da CONTRATANTE, assim como a infraestrutura externa, para a

implantação dos serviços contratados (passagem de cabos, lançamento de cabos ou fibras ópticas, adaptação de tomadas, etc.).

4.3.3. Da Disponibilidade dos Serviços de Acesso à Internet:

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

4.3.3.2. Caso haja necessidade técnica de interrupção provisória dos serviços, inclusive em função de mudança de tecnologia, a Contratada deverá comunicar o fato por escrito, com antecedência mínima de 7 (sete) dias úteis; podendo ser deferido ou não o pedido, dependendo da conveniência e interesse da Contratante, considerada a necessidade dos serviços de conexão à internet para o funcionamento das unidades administrativas e para manutenção de serviços WEB realizados pelo órgão;

4.3.3.3. As interrupções programadas mencionadas no subitem acima deverão ocorrer, preferencialmente, em finais de semana ou fora do horário comercial. Porém, importa destacar que, caso a Contratada exceda o período previsto, o referido serviço será considerado indisponível no tempo excedente, estando sujeito a glosas no faturamento mensal, sem prejuízo da possibilidade de aplicação de penalidades administrativas;

4.3.3.4. 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 Contratada;

4.3.3.5. Os níveis mínimos de serviços especificados pela Contratante considerarão a continuidade das atividades que dependem especificamente do acesso à internet para a qualidade no atendimento prestado aos assistidos da Contratante.

4.3.4. O Backbone do prestador de serviço de link dedicado deverá:

4.3.4.1. Possuir canais próprios e dedicados;

4.3.4.2. Garantido o funcionamento do serviço DNS a partir de servidores localizados nas dependências do Coren-SP, incluindo autoridade sobre as zonas diretas e reversas;

4.3.4.3. O serviço DNS deverá suportar o protocolo DNSSEC;

4.3.4.4. Possuir política de roteamento que permita trânsito nacional e internacional para a Contratante;

4.3.4.5. 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;

4.3.4.6. 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 duas interfaces Ethernet Full - Duplex (100/1000 Base- T);

4.3.4.7. Suportar o gerenciamento por SNMP (versões 1, 2 ou 3);

4.3.4.8. Suportar a coleta de estatísticas via SSFlow ou NetFlow;

4.3.4.9. Os protocolos SNMP, SFlow/NetFlow devem ser configurados para enviar estatísticas para sistemas internos à CONTRATANTE.

4.3.5. A Contratada deverá fornecer link único, não sendo aceito fornecimento de diversos links de menor velocidade com balanceamento entre eles;

4.3.6. Em locais que não for possível atender com fibra ótica, poderá ser atendido com IP dedicado com velocidade mínima de 50%, de acordo com a velocidade pedida para o local. Esse quantitativo não deverá ultrapassar 10% do quantitativo total de links a serem instalados considerado todo o objeto de contratação.

4.3.7. A Contratada deverá possuir Termo de Autorização da Agência Nacional de Telecomunicações – ANATEL, bem como o registro de suas estações;

4.3.8. Os serviços de acesso à internet não deverão sofrer nenhum tipo de tarifação adicional.

4.4. DO SERVIÇO DE ANTI-DDoS PARA O LINK DE 300 MBPS

4.4.1. A Contratada deverá possuir infraestrutura própria de mitigação com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional;

4.4.2. Entenda-se por infraestrutura própria de mitigação, a existência de equipamentos instalados no backbone da Contratada com o objetivo de bloquear o tráfego malicioso, evitando. Assim. a saturação da banda da internet e indisponibilidade dos serviços em momentos de ataques DDoS (Distributed Denial of Service);

4.4.3. Não serão aceitas soluções que contemplem equipamentos de mitigação no ambiente da Contratante, de forma que toda a infraestrutura de mitigação deverá ser instalada obrigatoriamente no backbone da Contratada;

4.4.4. A Contratada deverá possuir, pelo menos, 2 (dois) centros de limpeza, cada um com capacidade de mitigação de 40 Gbps (quarenta gigabits por segundo);

4.4.5. A Contratada deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e com quantidade ilimitada de eventos de ataque ao longo da vigência contratual;

4.4.6. O ataque deverá ser mitigado separando o tráfego legítimo do tráfego malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis. A técnica Anti-DDoS utilizada deverá ser por métrica de volumetria, não podendo haver restrições por volume de tráfego, devendo contemplar o volume total do link concentrador;

4.4.7. O serviço de 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;

4.4.8. Não deverá haver cobrança de taxa adicional por volume de mitigação de ataque nos IPs monitorados;

4.4.9. A Solução deverá 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;

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

4.4.11. Em eventuais ataques não detectados pela Contratada, quando identificados pela Contratante, estes deverão ser mitigados imediatamente pela Contratada após a abertura de chamado via central de suporte, sendo sempre considerado um chamado de Severidade Nível 1, devendo realizá-lo sem nenhum ônus à CONTRATANTE;

4.4.12. A Solução deverá manter uma lista dinâmica de endereços IPs bloqueados, retirando da lista os endereços que não enviarem mais requisições maliciosas, após um período de tempo considerado seguro pela Contratada e Contratante;

4.4.13. A Solução deverá implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

4.4.13.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

4.4.13.2. Ataques à pilha TCP, incluindo mau uso das Flags TCP, ataques de RST e FIN, SYN FLOOD e TCP IDLE RESETS;

4.4.13.3. Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

4.4.13.4. Ataques de botnets, worms e ataques que utilizam falsificação de endereços de origem (IP Spoofing).

4.4.14. Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de borda da Contratada;

4.4.15. A Solução deverá permitir a proteção, no mínimo, todo o tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;

4.4.16. A Contratada deverá disponibilizar, por meio eletrônico ou portal na internet, relatórios mensais de mitigação de ataques contendo, no mínimo, horário de início de ação de mitigação, horário de sucesso da mitigação e horário do fim do ataque;

4.4.17. Toda a conexão entre o backbone da Contratada e os equipamentos a serem instalados por nas dependências da Contratante, serão de exclusiva responsabilidade da Contratada;

4.4.18. Os equipamentos fornecidos pela Contratada deverão dar suporte a serviços de registro de nomes dinâmicos;

4.4.19. A interface entre o sistema instalado pela Contratada e a rede/equipamentos da Contratante deverá ser feita por meio de portas de comunicação do tipo RJ-45, via padrões 802.3u ou 802.3ab, compatível com a rede existente, sendo que, no mínimo, uma porta deverá às especificações;

4.4.20. Deverão ser fornecidos endereços de rede correspondentes aos protocolos IPv4 e IPv6. No caso do Ipv4, deverá ser fornecido, no mínimo, 1 (um) número de endereço Ipv4 (Internet Protocol) fixo e válido. Os IPs não poderão ser traduzidos por NAT até o backbone da operadora;

4.4.21. Caso haja necessidade por parte do CONTRATANTE, a CONTRATADA deverá executar configurações adicionais de roteamentos em seus equipamentos para funcionamento de sistemas informatizados, como por exemplo: relógio eletrônico.

4.5. DOS REQUISITOS DE GERÊNCIA DE REDE

4.5.1. 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 níveis de serviços.

4.5.2. As seguintes funcionalidades relacionadas à Gerência de Rede deverão ser atendidas pela Solução ofertada:

4.5.2.1. Disponibilizar a visualização de informações online (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

4.5.2.2. Atuar de forma proativa, antecipando os problemas na rede e garantindo o cumprimento dos SLAs estabelecidos, realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando 24 horas por dia, 7 dias por semana, todos os dias do ano;

4.5.2.3. 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;

4.5.2.4. Viabilizar a operação e administração através de uma console única, de forma que não serão aceitas soluções que possuam acessos segmentados aos módulos;

4.5.2.5. Dispor de escalabilidade, permitindo futuras ampliações no número de elementos de rede a serem gerenciados;

4.5.2.6. Permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc.;

4.5.2.7. Permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

4.5.2.8. A Solução de Gerência da Rede deverá ser 100% web sem a necessidade de instalação de clientes específicos. Logo, não serão aceitas soluções que não sejam nativas em WEB ou que requeiram a instalação de agentes ou plugins nos desktops dos empregados da Contratante;

4.5.2.9. Realizar acesso via web padrão HTTP e possuir suporte a HTTPS, devendo ser acessível através dos principais browsers do mercado, tais como Google Chrome, Mozilla Firefox, Microsoft Edge e Safari;

4.5.2.10. Possuir interface em língua portuguesa;

4.5.2.11. Permitir a exportação das informações para relatórios em formatos comerciais;

4.5.2.12. 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:

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.

São Paulo, 15 de junho de 2023.

CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

INTEGRANTE REQUISITANTE/ RESPONSÁVEL PELA ÁREA TÉCNICA (GTI)	INTEGRANTE TÉCNICO
Rafael Conceição da Silva Assinado de forma digital por Rafael Conceição da Silva Dados: 2023.06.15 16:04:55 -03'00' **Rafael Conceição da Silva** Gerente – GTI Matrícula 455	Regis de Oliveira Araujo Assinado de forma digital por Regis de Oliveira Araujo Dados: 2023.06.15 16:00:45 -03'00' **Régis de Oliveira Araújo** Analista de Segurança da Informação Matrícula 1044
INTEGRANTE DA ÁREA DE APOIO ADMINISTRATIVO	
Henrique Pereira Soares Assessor II – GAB/PRES Matrícula 975	