RELATÓRIO DE ESTUDO TÉCNICO PRELIMINAR - ETP

Base legal: Lei Federal nº 14.133/2021

ÁREA DEMANDANTE/SIGLA
SEÇÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO/SECITI
PREVISÃO NO PLANEJAMENTO ANUAL DE CONTRATAÇÕES (Número do Documento de Formalização de Demanda)
2025/135

1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO E ESTIMATIVA DAS QUANTIDADES (art. 18, §1º, incisos I e IV da Lei Federal nº 14.133/2021)

As atividades desenvolvidas na Câmara Municipal de Belo Horizonte (CMBH) demonstram uma significativa dependência de recursos de tecnologia da informação. Estes têm a capacidade de automatizar processos, incluindo o próprio processo legislativo, resultando em maior agilidade no atendimento aos interesses da sociedade belo-horizontina. Diversos arquivos são armazenados e sistemas são executados por meio deles, que fazem parte do dia a dia da atividade da CMBH. Isso inclui a gestão do processo legislativo, o apoio às atividades parlamentares, os processos administrativos, bem como as ferramentas de comunicação e divulgação, como o webmail e o portal.

Para garantir a proteção das informações geradas e armazenadas na infraestrutura tecnológica mencionada acima, a CMBH adquiriu em 2018 uma solução de Next Generation Firewall (NGFW). A solução é composta por 2 (dois) appliances físicos (Palo Alto PA-3020) em esquema de redundância com objetivo de garantir a disponibilidade do sistema. Ou seja, caso 1 (um) appliance falhe em algum momento, o outro mantém a infraestrutura em funcionamento, até que o problema seja sanado.

Conforme informações no site do fabricante (https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates), o suporte ao hardware da solução atual entrará em fase de End Of Life em 31/10/2024. Isso significa que o produto não receberá mais atualizações de segurança, correções de bugs ou suporte técnico do fabricante. Sendo assim, se faz necessária a abertura de novo processo licitatório

para substituição da solução atual.

O NGFW é uma solução avançada de segurança de rede que vai além das capacidades dos firewalls tradicionais. Enquanto os firewalls tradicionais focam principalmente no filtro de pacotes com base nos endereços IP de origem e destino, números de porta e protocolos, os NGFWs incorporam recursos adicionais para aprimorar a segurança e o controle da rede. Esses recursos incluem:

- **Filtro de conteúdo:** Controlar o acesso à Internet, oferecendo proteção eficiente contra conteúdos maliciosos, inadequados, ilegais e/ou improdutivos.
- **Controle de aplicação:** identificar e controlar dados na camada de aplicação, permitindo que administradores definam políticas baseadas em aplicativos específicos ou categorias de aplicativos. Esse controle granular ajuda a evitar que aplicativos não autorizados acessem a rede e visa melhorar a segurança geral.
- **Sistema de Prevenção de Intrusões (IPS):** monitorar o tráfego de rede em tempo real e analisar os pacotes de dados que circulam pela rede em busca de padrões ou comportamentos suspeitos que possam indicar atividades maliciosas.
- **Controles baseados em usuário:** integrar a sistemas de autenticação, como o Active Directory, permitindo que administradores criem regras com base em usuários ou grupos de usuários específicos. Isso garante que o acesso a determinados recursos seja restrito apenas a pessoas autorizadas.
- **Proteção Avançada contra Ameaças:** disponibilizar recursos de proteção avançada contra ameaças, como antivírus, antimalware, sandboxing e laboratórios de inteligência de ameaças. Esses recursos ajudam a identificar e bloquear ameaças sofisticadas que podem contornar medidas de segurança tradicionais.
- **Inspeção SSL:** inspecionar o tráfego criptografado (por exemplo, HTTPS) para detectar e prevenir ameaças ocultas em conexões criptografadas SSL/TLS. Isso é crucial, uma vez que muitas ameaças modernas usam criptografia para evitar sua detecção. Com esse recurso o firewall pode abrir sessões criptografadas e analisar o conteúdo em busca de ameaças, como o ransomware e outras.
- **Qualidade de Serviço (QoS):** priorizar o tráfego de rede com base em regras predefinidas, garantindo que aplicativos críticos recebam a largura de banda necessária e reduzindo o risco de problemas de desempenho.
- **Suporte a Rede Privada Virtual (VPN):** suporte à funcionalidade VPN integrada para segurança de conexões remotas e acesso seguro a redes

corporativas. A VPNs podem ser através de conexão entre redes distintas (site-to-site) ou permissão de acesso de usuários à uma rede corporativa (client-to-site).

- **Gerenciamento centralizado:** possuir consoles de gerenciamento centralizado, permitindo que administradores configurem, monitorem e gerenciem políticas de segurança e dispositivos a partir de uma única interface.
- **Alta disponibilidade:** capacidade de um sistema, serviço ou aplicação de estar constantemente disponível e operacional, mesmo em face de falhas ou interrupções inesperadas.

A integração desses recursos proporciona uma melhor visibilidade do tráfego de rede e proteção aprimorada contra uma ampla variedade de ameaças cibernéticas, tornando o NGFW um componente elementar para a infraestrutura de segurança de rede da CMBH.

Considerando que a solução atualmente utilizada pela CMBH já se trata de um Next Generation Firewall, este estudo será conduzido no sentido de manter, no mínimo, os requisitos de segurança já empreendidos até aqui. Sendo assim, iremos avaliar os modelos de contratação disponíveis, com o objetivo de identificar qual proporcionará a maior elevação do nível de maturidade da CMBH em segurança da informação.

Quantitativos:

Há a necessidade de segurança e disponibilidade da solução, razão pela qual 2 (dois) equipamentos de firewall devem ser ofertados. Caso 1 (um) equipamento falhe em algum momento, o outro deverá manter a infraestrutura em funcionamento, até que o problema seja sanado. Os equipamentos deverão ser acompanhados de todos os acessórios necessários para o funcionamento da solução de NGFW em alta disponibilidade.

Há necessidade de licenciamento completo para diversas funcionalidades, como tratamento de ameaças, filtro de URL, atualizações de software da solução, dentre outros, sendo parte integrante desta, para gerenciamento e controle, monitoramento, e demais operações a serem realizadas pela SECITI. Precisam ser adquiridos uma única vez, com período de validade definido de 12 (doze) meses.

Também será contratado 1 (um) serviço de implantação e migração da solução, e 1 (um) serviço de treinamento e operação assistida, que necessitam ser utilizados apenas uma única vez, após a solução implantada.

Além disso, deverá ser contratado 12 (doze) meses de serviços de suporte técnico e garantia, que é tempo igual a vigência do contrato.

As quantidades e especificações detalhadas de cada item foram determinadas após avaliação do cenário atual da CMBH, que se mostrou adequado, e com possibilidade de suportar falhas.

2 - LEVANTAMENTO DE MERCADO (art. 18, §1º, inciso V da Lei Federal nº 14.133/2021 e art. 22, §1º, inciso I da Portaria da CMBH nº 20.453/2022)

Após análise do mercado, identificamos as seguintes opções para contratação da solução deste estudo:

Solução 1: Aquisição de Infraestrutura de NGFW

A aquisição da infraestrutura de Firewall consiste na compra de todos os componentes (hardware e software) necessários para a implantação da solução. Isso significa a incorporação dos bens ao patrimônio da CMBH.

Vantagens:

- Controle interno dos ativos de segurança (hardware e software);
- Custo tende a se tornar mais vantajoso a médio prazo;
- Mitigação do risco de quebra de contrato, uma vez que os equipamentos da solução serão incorporados ao patrimônio da CMBH.
- Conceder a total e completa gestão da segurança de rede de dados para a COOTEC.
- As funcionalidades essenciais da solução adquirida continuam em funcionamento mesmo após o fim da vigência das licenças contratadas.

Desvantagens:

- Necessidade de adquirir novos equipamentos após o EoF para manter todas as funcionalidades ativas;
- Curva de aprendizado da equipe interna na utilização da ferramenta.

Solução 2: Firewall como Serviço (FWaaS)

O Firewall as a Service (ou outsourcing de firewall) define a locação de toda solução atrelada ao gerenciamento e à manutenção da ferramenta. Isso significa que a CMBH não realizaria a aquisição de um ou mais equipamentos (hardware), mas sim, a contratação de um serviço que prevê a instalação de todos os equipamentos necessários para o funcionamento da solução. Neste modelo de contratação estão

embarcados os serviços de implementação e manutenção da ferramenta. Desta maneira, além da disponibilização da ferramenta, a CMBH contará também com o suporte técnico de equipe especializada na solução para realizar a gestão ativa do sistema.

Vantagens:

- Possibilidade de atualizar o hardware (appliance) ao longo do contrato, caso o mesmo atinja o EoF.

Desvantagens:

- Risco de finalização do contrato: os equipamentos são da empresa e ela poderá retirá-los nos casos de quebra/fim da vigência contratual.
- É necessário realizar as contratações subsequentes sem quebra na continuidade do serviço, uma vez que, por ser um serviço essencial, não é possível que a CMBH suspenda sua operação em caso de estar com os equipamentos em comodato.

3 - JUSTIFICATIVA TÉCNICA E ECONÔMICA DA SOLUÇÃO ESCOLHIDA (art. 18, §1º, inciso V da Lei Federal 14.133/2021)

Conforme pode ser conferido no levantamento de mercado, a Solução 1 - Aquisição da Infraestrutura de NGFW – se mostrou a opção mais vantajosa tanto técnica quanto economicamente.

Ao contrário do que foi previsto ao iniciar este estudo, a contratação do NGFW como serviço (Solução 2) não indica a disponibilidade contínua de equipamentos de última geração. Durante as reuniões com os fornecedores foi identificado que as empresas, de modo geral, não realizam a substituição dos equipamentos instalados no início dos serviços, a menos que esta atualização esteja prevista em contrato. Contudo, a inclusão desta exigência no TR, implica o aumento significativo do valor agregado do serviço. Sendo assim, a obsolescência de um hardware pode ocorrer tanto na contratação pela Solução 1, quanto pela Solução 2.

Além disso, na Solução 2 também foram identificados riscos de descontinuidade dos serviços durante a substituição de fornecedor proveniente da quebra/finalização da vigência contratual. Este risco não ocorre na Solução 1 porque, por padrão, as funcionalidades essenciais do Firewall são perpétuas, garantido a continuidade do serviço independente da atualização das assinaturas de renovação anual.

A questão de proficiência da equipe na operação da ferramenta, pode ser atendida com a contratação de suporte técnico especializado. Este serviço pode ser contratado independente do tipo de contratação definido.

E por fim, a avaliação das propostas dos fornecedores demonstrou que a Solução 1 é economicamente mais vantajosa, conforme apresentado na tabela do item 4, pois inclui a compra dos equipamentos. Embora a média calculada para a Solução 1 seja superior ao valor médio da Solução 2, a Solução 1 inclui a incorporação de todos os equipamentos ao patrimônio da CMBH. Isso mitiga o risco de descontinuidade contratual, pois, ao adquirir os equipamentos, a CMBH garante seu funcionamento com as últimas atualizações, sem comprometer a operação da instituição. Esse é o modelo atualmente utilizado pela casa.

Por outro lado, a Solução 2, que se baseia no aluguel dos equipamentos, apresenta o risco de descontinuidade contratual, uma vez que os equipamentos seriam retirados, o que comprometeria toda a segurança da rede, potencialmente causando uma interrupção completa dos serviços de Tecnologia da Informação. Logo, dado o risco elevado em caso de eventual descontinuidade contratual, a solução 2 revela-se tecnicamente inviável e desvantajosa para a CMBH.

Feita a prévia consulta ao mercado, e escolhida a solução, fica abaixo consolidada a planilha com a previsão dos itens, unidades e quantidades que futuramente serão registrados no Termo de Referência.

Nº LOTE	Nº DO ITEM	DESCRIÇÃO DO ITEM	UNIDADE	QUANTIDADE
1	1	Appliance físico - Next Generation Firewall (NGFW)	Unidade	2(dois)
	2	Licenciamento de softwares da solução de Next Generation Firewall - NGFW	Unidade	1(um)
	3	Serviço de implantação e migração	Unidade	1(um)
	4	Serviço de treinamento e operação assistida	Unidade	1(um)

	5	Serviço de suporte técnico e garantia	Mês	12(doze)

4 - ESTIMATIVA DO VALOR DA CONTRATAÇÃO (art. 18, §1º, inciso VI da Lei Federal nº 14.133/2021 e art. 25 da Portaria da CMBH nº 20.453/2022)

Para embasar a solução definida por este ETP, foram analisadas 03 soluções líderes de mercado no segmento de NGFW. Após o contato com os fornecedores, foi solicitado orçamento prévio das soluções (ANEXO I - ESTIMATIVA DO VALOR DA CONTRATAÇÃO) de acordo com as necessidades atuais da CMBH. Esses fornecedores foram consultados em razão da existência de contratos pretéritos com a CMBH ou em função de buscas por parceiros de três fabricantes distintos, com o objetivo de demonstrar que não há qualquer direcionamento nas especificações. Esse número de fornecedores reflete uma variação de marcas e modelos com a amplitude necessária para o levantamento de mercado. O resumo das cotações pode ser conferido na tabela abaixo:

Código	Solução 1	Solução 2		
	Total Anual	Meses	Total Mensal	Total Anual
Fornecedor 1	509.282,37	12	50.252,90	603.034,80
Fornecedor 2	795.900,00	12	48.431,00	581.172,00
Fornecedor 3	1.367.594,00	-	-	-
Média	652.591,19*			592.103,40

*O cálculo da média desconsiderou o total anual do Fornecedor 3, uma vez que ele oferece somente a Solução 1 e o valor da proposta mostra-se extremamente superior às propostas dos fornecedores 1 e 2.

A partir das informações constantes da proposta, foi necessário promover alguns ajustes para equalizá-las. Dessa forma, foi considerado sempre o período de 12 meses em relação aos custos ofertados. Quando os fornecedores apresentaram propostas para 36 meses, o custo foi dividido por ano, de modo a permitir a comparação dos valores.

O presente estudo identificou que existe a possibilidade de contratações por 12 ou 36 meses. Esse prazo influencia diretamente no período de validade das licenças da solução e garantia (itens 2 e 5). Após análise, conclui-se que a contratação por 12

meses para esse objeto é tecnicamente mais vantajosa para a CMBH, uma vez que é comum a descontinuidade do modelo do appliance (equipamento) em periodicidade que não pode ser antecipadamente prevista. Uma contratação por 36 meses pode inviabilizar a manutenção da solução como um todo, no sentido de prejudicar o investimento em tempo e capacitação dos servidores para domínio da ferramenta, bem como no risco de continuamente modificar a tecnologia adotada pela CMBH, maior dificuldade em gestão e fiscalização contratual e gasto com novos processos licitatórios. Por exemplo: considerando que o fabricante dê suporte à solução por 60 meses, com uma contratação por 36 meses é inviável realizar a renovação das licenças e garantia (itens 3 e 5) em período fracionado ao estipulado (24 meses), e portanto seria necessário novo processo licitatório, ainda que a solução adquirida pudesse ser aproveitada com suas licenças e garantia renovadas por mais 24 meses no caso do contrato ter vigência anual. Assim, com a vigência anual, espera-se a permanência da solução por um tempo maior no ambiente da CMBH do que em uma contratação por 36 meses que poderá não vir a ser renovada pelo descasamento entre o prazo de descontinuidade do modelo e a duração do contrato.

Ressalta-se que essa estimativa da contratação é feita por um procedimento simplificado, nos termos do art. 25 da Portaria CMBH nº 20.453/2022, que dispõe que: "A estimativa do valor da contratação no estudo técnico preliminar será baseada em pesquisa simplificada de mercado, sem que se exija o mesmo rigor metodológico da orçamentação definitiva, a fim de realizar o levantamento do eventual gasto com a solução escolhida e de verificar a viabilidade econômica da opção."

Logo, o valor estimado da contratação somente será obtido após a confecção do TR com a sua consequente submissão ao mercado na etapa da pesquisa de preços.

5 - DESCRIÇÃO DA SOLUÇÃO (art. 18, §1º, VII da Lei Federal nº 14.133/2021):

5.1 - Condições gerais e específicas de execução e aceitação do objeto ou padrões mínimos de qualidade para o serviço a ser contratado:

A solução ofertada deverá atender na plenitude a todos os requisitos mínimos estabelecidos e às demais condições que serão previstas no edital, em seus anexos e subanexos.

Os requisitos de hardware e software dos itens que compõem a solução de firewall serão descritos no “**Subanexo A - Requisitos de hardware e software**”.

A dinâmica e requisitos do serviço de implantação e migração serão descritos no “**Subanexo B - Dinâmica e requisitos de implantação e migração**”.

As características do serviço de treinamento e operação assistida na solução pela contratada serão descritos no **"Subanexo C - Treinamento e operação assistida"**.

As características do serviço de suporte técnico e garantia na solução pela contratada serão descritos no **"Subanexo D - Suporte técnico e garantia"**.

Os serviços de implantação e migração, treinamento, suporte e operação assistida deverão ser realizados por pessoal técnico da CONTRATADA, com experiência e conhecimentos na solução ofertada.

A CMBH e a CONTRATADA, após a assinatura do contrato, realizarão reunião de *kick-off* em dia e horário a serem combinados entre as partes. Nesta reunião, a CONTRATADA deverá apresentar o cronograma de entrega e implantação da solução, nos prazos definidos no termo de referência, apresentando ainda os profissionais envolvidos, e o preposto designado.

CONDIÇÕES DE ACEITE E RECEBIMENTO

Observados os prazos estabelecidos para a entrega dos equipamentos e prestação dos serviços no tópico **12 - Informações Adicionais**, a CMBH efetuará o recebimento provisório do objeto, para efeito de posterior verificação de sua conformidade com a especificação do edital, quanto aos aspectos de qualidade e quantidades contratadas, após o que promoverá seu recebimento definitivo.

5.1.1 Para o item 1 da tabela, a CMBH receberá provisoriamente, no ato da entrega, os equipamentos da solução, tais como maquinário, cabos, conectores, acessórios, peças e demais itens, mediante emissão de termo de recebimento ou assinatura de nota de simples remessa. O recebimento definitivo ocorrerá após a solução estar completamente em produção (equipamentos em pleno funcionamento, licenças ativas, implantação e migração concluídas), no prazo de 10 dias úteis.

5.1.2 Para o item 2 da tabela, a CMBH receberá de forma definitiva o item quando comprovada a ativação do licenciamento, e ativação da garantia pelos prazos e condições estabelecidas no termo de referência, após ou durante a implantação da solução, por meio de verificação das licenças em site do fabricante, ou outro meio equivalente, e verificação da disponibilidade das funcionalidades exigidas. Não há recebimento provisório para este item.

5.1.3 Para os itens 3 e 4, o recebimento definitivo será efetuado pela CMBH quando estes serviços forem concluídos, nas condições e requisitos estabelecidos no

termo de referência, e verificação de que os mesmos atendem a todos os requisitos estabelecidos. Não há recebimento provisório para estes itens.

5.1.4 Para o item 5, o recebimento provisório será consubstanciado no ateste do fiscal da correta execução do serviço, quando da emissão da nota fiscal, considerando-se definitivamente recebido com a liquidação da nota fiscal pelo gestor.

5.1.5 O recebimento provisório compete ao fiscal e o definitivo ao gestor, e o recebimento dos bens a que compõem a solução caberá a comissão composta por pelo menos 3 (três) servidores da CMBH, indicados por ato do Coordenador de Informática para acompanhamento e fiscalização da contratação decorrente deste termo de referência, sendo facultado à CONTRATADA a participação de um ou mais de seus colaboradores, que deverão ter conhecimento técnico para a conferência.

5.1.6 Constatada qualquer irregularidade, pendência, ou ocorrendo demais problemas durante a execução do contrato, os mesmos serão levados ao conhecimento da CONTRATADA, a qual deverá providenciar a correção desses problemas, promovendo sua adequação às exigências definidas em contrato.

5.1.7 O objeto contratado será rejeitado caso esteja em desacordo com as especificações, devendo a CMBH apontar esta ocorrência por escrito, onde serão detalhadas as razões para deixar de emitir o termo de recebimento definitivo e indicará as falhas e pendências verificadas, bem como o prazo para sua resolutividade.

5.1.8 O recebimento definitivo do objeto não exclui nem reduz a responsabilidade da CONTRATADA com relação ao funcionamento e às configurações divergentes do especificado, durante todo o seu período de garantia.

5.1.9 Em caso de rejeição total/parcial do objeto contratado ou demais hipóteses de descumprimento de outras obrigações contratuais, avaliadas na etapa de recebimento, a CONTRATADA estará sujeita à aplicação de sanções administrativas cabíveis, observados os procedimentos legais pertinentes.

PROPRIEDADE, SIGILO E RESTRIÇÕES

5.1.10 A CONTRATADA é integralmente responsável pela manutenção de sigilo sobre quaisquer dados, informações e artefatos contidos em documentos e em mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto e forma, divulgar, reproduzir ou utilizá-los para outros fins que não os vinculados diretamente aos serviços prestados à CMBH.

5.1.11 A CONTRATADA fica obrigada a obedecer às políticas e normas adotadas pela CMBH.

5.1.12 A CONTRATADA não poderá repassar a terceiros, em nenhuma hipótese, quaisquer informações sobre a infraestrutura tecnológica da CMBH, assim como sobre dados e metadados, configurações, arquitetura, dentre outros, devendo manter a segurança das informações dos componentes da solução como um todo.

5.1.13 A CONTRATADA obriga-se a observar os ditames da Lei Geral de Proteção de Dados Pessoais (LGPD).

DEVERES E RESPONSABILIDADES DA CMBH

5.1.14 Fiscalizar o perfeito cumprimento do objeto e das demais cláusulas do edital e do contrato.

5.1.15 Comunicar tempestivamente à CONTRATADA, por escrito, sobre as possíveis irregularidades observadas nos bens ou no decorrer da prestação dos serviços, para a imediata adoção das providências de modo a sanar os problemas eventualmente ocorridos.

5.1.16 Proporcionar as condições necessárias para que a CONTRATADA possa cumprir o estabelecido no edital e no contrato.

5.1.17 Atestar as notas fiscais que tenham sido entregues como determina o contrato, verificar os relatórios apresentados e encaminhar as notas fiscais, devidamente atestadas, para pagamento dentro do prazo determinado.

5.1.18 Notificar a CONTRATADA, por escrito, sobre eventuais imperfeições, falhas, e demais irregularidades verificadas na execução dos procedimentos previstos no edital e no contrato, de modo a que possam ser adotadas medidas para correção do que for notificado.

5.1.19 Efetuar os pagamentos no prazo e nas condições indicadas neste instrumento, após a assinatura do termo de recebimento definitivo, e comunicar à CONTRATADA quaisquer irregularidades ou problemas que possam inviabilizar os pagamentos.

5.1.20 Fornecer, em tempo hábil, todos os dados técnicos e informações de sua responsabilidade, necessários à execução do objeto do contrato.

5.1.21 Informar à CONTRATADA da presença de profissionais que não possuem o conhecimento técnico e a postura profissional necessária à perfeita realização dos serviços.

5.1.22 Rejeitar, no todo ou em parte, os serviços prestados em desacordo com o contrato.

5.1.23 Prestar informações e esclarecimentos solicitados pela CONTRATADA sobre os serviços.

5.1.24 Modificar unilateralmente o contrato para melhor adequação das finalidades do interesse público, respeitados os direitos da CONTRATADA e as disposições legais pertinentes.

DEVERES E RESPONSABILIDADES DA CONTRATADA

5.1.25 Manter, durante a execução do objeto, todas as condições estabelecidas no edital e em seus anexos, bem como aquelas estabelecidas no contrato.

5.1.26 Responsabilizar-se pelo integral cumprimento do contrato, arcar com os eventuais prejuízos causados à CMBH ou a terceiros, provocados por ineficiência na prestação dos serviços, respondendo integralmente pelo ônus daí decorrente, o que não exclui nem diminui sua responsabilidade por aqueles danos que se evidenciarem, independentemente do controle e da fiscalização exercidos pela CMBH.

5.1.27 Entregar os produtos livres de defeitos e de acordo com as exigências contidas na legislação vigente, obrigando-se a substituir/corrigir/reparar, de imediato, qualquer produto entregue com defeito.

5.1.28 Fornecer as devidas notas fiscais nos termos da lei e cumprir todas as obrigações fiscais decorrentes da execução do contrato, responsabilizando-se pelas infrações fiscais daí advindas.

5.1.29 Prestar as informações e os esclarecimentos relativos ao objeto da contratação, quando solicitados pelos agentes designados pela CMBH.

5.1.30 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos valores de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos.

5.1.31 Arcar com todos os custos inerentes à prestação dos serviços e ao seu fornecimento, tais como deslocamento, alimentação, recursos, transporte, alojamento, trabalho aos sábados, domingos, feriados ou em horário noturno, ou com qualquer outro valor adicional.

5.1.32 Prover identificação (crachá) aos seus colaboradores, que deverá ser utilizado durante a permanência nas dependências da CMBH, segundo as normas de segurança desta.

5.1.33 Observar, durante a realização do trabalho e para os produtos a serem entregues, todas as leis, decretos, normas, portarias, instruções normativas a que esteja submetida a CMBH.

5.1.34 Designar um Preposto, que será o responsável por toda a comunicação a ser

feita com a CMBH.

5.1.35 Possuir, quando do início dos trabalhos, suporte técnico disponível para atendimento à CMBH em face de eventuais necessidades específicas, de forma a garantir os níveis de SLA ou facilitar intermediações entre o implantador e o fabricante da solução contratada.

5.1.36 Comunicar à CMBH qualquer substituição dos profissionais envolvidos na execução do objeto deste termo de referência, independente do motivo, seja ele temporário ou definitivo.

5.1.37 Fazer cumprir as normas de segurança e medicina do trabalho, responsabilizando-se por qualquer acidente que venha a ocorrer durante a execução dos serviços contratados.

5.1.38 Prestar, obrigatória e imediatamente, esclarecimentos às solicitações requeridas pelo responsável da CMBH pelo acompanhamento e fiscalização operacional da execução do contrato.

5.1.39 Não permitir que os prazos dos serviços excedam os prazos definidos neste Termo de Referência, e tampouco o prazo de vigência do contrato.

5.1.40 O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela CONTRATADA, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, podendo culminar em rescisão contratual, conforme disposições contidas na Lei Federal nº 14.133/2021.

DO REGISTRO DE OPORTUNIDADE

5.1.41 Não serão aceitas as propostas comerciais das LICITANTES que realizem a prática de Registro de Oportunidade para o presente objeto. Tal exigência está em compatibilidade com o Parecer PROLEG – nº 11/2021, referente ao processo nº 1.487/2020, e visa atender ao princípio da isonomia e ampla competitividade do certame, em consonância com o art. 11 da Lei 14.133/2021.

REQUISITOS DA PROPOSTA COMERCIAL

5.1.42 Para fins de análise da compatibilidade técnica do objeto ofertado com as especificações do termo de referência, a LICITANTE deverá apresentar, junto a proposta comercial e como requisito de aceitabilidade desta, documentação que demonstre os requisitos técnicos de cada um dos itens ofertados.

5.1.43 Entende-se como documentação para estes fins os prospectos técnicos, catálogos, manuais, folders, datasheets, ou qualquer outra documentação oficial da solução ofertada, em inglês ou português, que contenha e comprove que esta solução, seus equipamentos, softwares e acessórios, atendam a

todas as especificações técnicas deste termo de referência.

5.1.44 Será desclassificada a proposta da LICITANTE que tiver documentação da solução ofertada com especificações inferiores ou incompatíveis às exigidas neste Termo de Referência.

5.1.45 A proposta comercial deverá ser preenchida conforme modelo disponibilizado para tal, considerando o agrupamento de componentes da tabela do item 1.1, com os preços unitários de cada item, para a composição dos preços totais de cada item e do preço total global.

ALTERAÇÃO SUBJETIVA

5.1.46 É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da CMBH à continuidade da contratação.

DISPONIBILIDADE DE PESSOAL

5.1.47 Os serviços prestados pela Contratada deverão ser realizados por pessoal técnico certificado pelo fabricante da solução de Next Generation Firewall, devendo aquela comprovar, para celebração do contrato, que possui em seu quadro de funcionários pelo menos 1 profissional com tal certificação, sendo plenamente capaz de dar suporte e realizar todas as demais atividades necessárias ao pleno funcionamento da solução ofertada. Essa condição deve ser mantida durante toda a execução do contrato, e a qualquer tempo a CMBH poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas.

CARACTERÍSTICAS DO SUPORTE TÉCNICO

5.1.48 O serviço de suporte técnico a ser prestado pela CONTRATADA visa ofertar atenção à equipe técnica da CMBH para resolução de problemas e esclarecimento de dúvidas no uso, configuração e monitoramento da solução. É digno de nota que exige-se a prestação do serviço de suporte técnico da CONTRATADA, embora exista o conceito de responsabilidade solidária do fabricante. Assim, a CMBH se reserva ao direito de responsabilizar a CONTRATADA por eventuais serviços de suporte ou garantia não realizados pelo fabricante da solução.

5.1.49 O suporte técnico deverá contemplar a resolução de dúvidas, incluindo configurações dos equipamentos e seus softwares e sistemas instalados pela CONTRATADA ou de fábrica.

5.1.50 A CONTRATADA deverá garantir o pleno e correto funcionamento dos equipamentos e de todo o software instalado, prestando o serviço de suporte técnico especificado, durante toda a vigência do contrato, contados a partir da data em que a solução entrar completamente em produção (entrega definitiva, incluindo ativação das licenças).

5.1.51 Caso em uma demanda de suporte técnico seja constatado erro intrínseco da solução, ensejando manutenção corretiva, a CONTRATADA deverá providenciar o registro e proceder à correção e atualização, seguindo os SLAs estabelecidos.

5.1.52 Os incidentes serão classificados em tipo e nível de severidade, conforme tabela a seguir:

INCIDENTES - PROBLEMAS TÉCNICOS (configuração inadequada, erro de funcionamento da solução, falha em integração, etc.)		
SEVERIDADE	**PRAZO PARA SOLUÇÃO PROVISÓRIA**	**PRAZO PARA SOLUÇÃO DEFINITIVA**
CRÍTICO	2 horas	4 horas
ALTO	4 horas	24 horas
MÉDIO	24 horas	48 horas
BAIXO	48 horas	120 horas
DESCRIÇÃO DOS NÍVEIS DE SEVERIDADE		
CRÍTICO	Incidente com parada da solução ou componente relevante, ou comprometimento gravíssimo de dados, processos ou ambiente, que interrompam os trabalhos.	
ALTO	Incidente com parada parcial da solução ou componente relevante, ou comprometimento grave de dados, processos ou ambiente, que prejudiquem mas não interrompa os trabalhos.	
MÉDIO	Incidente sem parada da solução, mas com comprometimento de dados, processos ou ambiente.	
BAIXO	Incidente sem parada da solução, com pequeno ou nenhum comprometimento de dados, processos ou ambiente.	

OBS: Para os casos que necessitem troca ou reparo de componentes, equipamentos, ou acessórios, estes deverão ocorrer em no máximo 48 (quarenta e oito) horas.

5.1.53 As dúvidas de operação serão classificadas em tipo e nível de severidade, conforme a tabela:

DÚVIDAS DE OPERAÇÃO (dúvidas de configuração, manutenção e monitoramento; atualizações funcionalidades; etc.)	
SEVERIDADE	**PRAZO PARA SOLUÇÃO**
CRÍTICO	2 horas
ALTO	4 horas
MÉDIO	12 horas
BAIXO	24 horas
DESCRIÇÃO DOS NÍVEIS DE SEVERIDADE	
CRÍTICO	Dúvida que impeça a realização de configuração ou manutenção crítica para a CMBH, com altíssimo risco de comprometimento de segurança ou perda de dados.
ALTO	Dúvida que impeça a realização de configuração ou manutenção importante para a CMBH, com alto risco de comprometimento de segurança ou perda de dados.
MÉDIO	Dúvida que impeça a realização de configuração ou manutenção para operação da solução de maneira mais eficiente, com baixo risco de comprometimento de segurança ou perda de dados.
BAIXO	Demais dúvidas sobre a configuração, manutenção e monitoramento da solução ofertada, sem risco de comprometimento de segurança ou perda de dados.

5.1.54 Os prazos descritos começarão a contar a partir do registro do chamado, via Web, contato telefônico ou e-mail.

5.1.55 **O suporte técnico, sob demanda da CMBH, deverá estar disponível em horário integral, todos os dias da semana em regime de 24 x 7, para atendimento on-site, na sede da CMBH.** A critério da CMBH, poderá ser realizado atendimento remoto.

5.1.56 O registro de chamados no sistema de atendimento deverá ser permitido em qualquer horário.

5.1.57 Para os níveis de severidade CRÍTICO e ALTO, a CONTRATADA deverá retornar para a CMBH com previsão e demais orientações necessárias para

mitigar o incidente em, no máximo, 1 (uma) hora, a contar da abertura do chamado, por atendimento remoto. Caso a CMBH identifique nesta primeira interação a necessidade de atendimento on-site, a CONTRATADA deverá acionar a sua equipe, e informar o horário do atendimento presencial, para continuidade do suporte.

5.1.58 Considera-se como solução provisória do problema a correção, mesmo que paliativa, do mau funcionamento registrado.

5.1.59 Considera-se como solução definitiva do problema, a correção da situação que provocou o mau funcionamento registrado para que não ocorra mais.

5.1.60 A CONTRATADA deve garantir que, quando da execução dos serviços de suporte técnico remoto e presencial, repassará à equipe técnica da CMBH os conhecimentos teóricos e práticos que fundamentaram a solução dos problemas e a melhoria da plataforma, possibilitando em situações futuras a autonomia da equipe em questões similares.

5.1.61 Ao final de todos os atendimentos, a CONTRATADA deverá apresentar à CMBH o relatório técnico contendo data e horários de atendimento, todas as ações realizadas e documentadas, a causa raiz do problema, operações e configurações na solução, reparos realizados, e solução definitiva, podendo este ser registrado no sistema de atendimento. Este relatório servirá de base de conhecimento para a CMBH, em caso de novas ocorrências.

5.1.62 A CMBH poderá solicitar repetição do repasse do conhecimento, com os ajustes necessários, sem ônus adicional, caso a sua qualidade não atenda às expectativas.

5.1.63 Inclui-se no procedimento de repasse a elaboração pela CONTRATADA de documentação detalhada dos procedimentos executados para a guarda de registros para consultas futuras.

5.1.64 As ações realizadas pela CONTRATADA não poderão comprometer outras funcionalidades da solução, de outro software ou ambiente da CMBH.

5.1.65 Um incidente poderá ter seu nível de severidade alterado pela CMBH, para uma maior ou menor severidade, sendo a contagem dos prazos do novo nível reiniciada.

5.1.66 Em qualquer caso, a CONTRATADA deverá arcar com todos os procedimentos necessários à solução do problema, incluindo a substituição de quaisquer módulos defeituosos no(s) equipamento(s), reparos e configurações, bem como a substituição do(s) próprio(s) equipamentos(s), se for necessário.

Duração Inicial do Contrato: 12 meses, permitindo prorrogação por até 120 meses, conforme art. 106 c/c art. 107 da Lei 14.133/2021

6 - JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO (art. 18, §1º, inciso VIII da Lei Federal nº 14.133/2021)

A presente contratação será por:

( ) Item.

(X) Lote.

Justificativa para a escolha da contratação por item ou lote:

A licitação em lote é um mecanismo bastante correto, dentro do escopo da legislação aplicável, na medida em que torna mais vantajoso para as empresas disputarem o certame, evitando vitórias minimizadas que redundam em desinteresse no cumprimento posterior e em disputas supervenientes. Esclareça-se que a contratação dividida em itens do presente objeto não se mostra tecnicamente viável, com prejuízo para o conjunto ou complexo do objeto, perda de economia de escala e até mesmo risco de restarem frustrados itens importantes de menor valor.

O objeto é constituído de fornecimento de uma solução, composta por bens e serviços muito especializados, que estão fortemente relacionados entre si, devendo ser prestado por uma única empresa. Por exemplo, os serviços de suporte e treinamento deverão ser prestados para o bem adquirido, com marca e modelo específico, logo, não seria eficiente e econômico a divisão do objeto. Os itens especificados apresentam homogeneidade e isso propiciará também que se evite o excesso de contratações individualizadas.

Essa composição tem respaldo na observação da lógica do mercado deste tipo de solução, considerando as soluções passíveis de serem ofertadas por um conjunto de fornecedores e fabricantes que se dedicam à prestação do tipo de objeto. Destaca-se ainda a eficiência na gestão de contrato único, o que seria rigorosamente difícil em vários contratos para o objeto em tela. Por fim, o agrupamento dos itens afasta a incerteza do êxito da contratação de todos os itens no mesmo processo, sendo que

os itens são interdependentes e a ausência de um deles na contratação traria prejuízo imensurável para manter a solução em pleno funcionamento.

Adicionalmente, é prática de mercado a comercialização da solução completa, sendo recomendado pelos fabricantes que sejam utilizados somente componentes devidamente testados e homologados para funcionamento em ambiente conjunto, devido às suas especificidades. É estritamente necessário que os componentes sejam compatíveis entre si. Com a separação por itens, há o risco real de incompatibilidade entre os componentes, podendo tornar inviável a implantação da solução.

Conclui-se que é tecnicamente justificável a aquisição por lote único, atendendo ao princípio da padronização no inciso V, alínea 'a', art. 40 e inciso I art. 47 da Lei nº 14.133/21". Desta forma, justifica-se o agrupamento de itens relativos à aquisição de solução de Next Generation Firewall (NGFW), por ser medida mais adequada, eficiente e vantajosa para a Administração Pública.

7 - RESULTADOS PRETENDIDOS (art. 18, §1º, IX da Lei Federal nº 14.133/2021):

O resultado pretendido com a presente contratação é garantir a segurança perimetral da rede de dados da CMBH, de modo a manter a integridade, disponibilidade e confidencialidade das informações dos sistemas da Câmara Municipal de Belo Horizonte.

8 - POSSÍVEIS PROVIDÊNCIAS PARA ADEQUAÇÃO DA CMBH (art. 18, §1º, X da Lei Federal nº 14.133/2021)

Há necessidade de adoção de providências pela CMBH previamente à celebração do contrato?
(X) Não.

9 - CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES (art. 18, §1º, XI da Lei Federal nº 14.133/2021)

Há contratações correlatas e/ou interdependentes?
(X) Não.

10 - POSSÍVEIS IMPACTOS AMBIENTAIS (art. 18, §1º, XII da Lei Federal nº 14.133/2021)

Há possíveis impactos ambientais decorrentes da pretendida contratação (art. 18, §1º, XII da Lei Federal nº 14.133/2021)?
( ) Não.

(X) Sim. Serão descritas a seguir as respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável:

As especificações dos equipamentos contemplados pela solução foram estabelecidas com base em padrões que as fazem respeitar normas nacionais e internacionais de sustentabilidade.
Como exemplo, o padrão Green Ethernet, que significa que os equipamentos são dotados de tecnologia de economia de energia nos dispositivos de comunicação. Além disto, os equipamentos envolvidos neste tipo de objeto possuem conformidade com a diretiva de restrição de substâncias perigosas (Restriction of Hazardous Substances) RoHS, para que sejam menos nocivos ao meio ambiente. A CONTRATADA deverá observar ainda, para a execução do objeto, quando possível e naquilo que couber, os seguintes princípios básicos de sustentabilidade:
a) Racionalização do uso de substâncias potencialmente tóxicas/poluentes na implantação da solução;
b) Substituição de substâncias tóxicas por outras atóxicas ou de menor toxicidade na implantação da solução;
c) Uso de ferramental elétrico ou eletrônico que estejam devidamente regulados ou calibrados, para racionalização/economia no consumo de energia;
d) Triagem adequada dos resíduos gerados na execução do serviço, observadas as disposições legais e regulamentares;
e) Fornecimento de material e documentação em meio eletrônico, reduzindo totalmente o uso de papel quando possível.

11 - ELEMENTOS ADICIONAIS DO ESTUDO TÉCNICO PRELIMINAR (art. 22, incisos II, III, IV e V da Portaria 20.453/2022 da CMBH)

11.1 - Indicação da forma pela qual será realizada a fiscalização do contrato:

A conformidade do material adquirido deverá ser verificada juntamente com o documento da contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido no Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

Além disso, o fiscal também verificará a correta instalação e configuração dos equipamentos junto à contratada.

Por fim, o fiscal promoverá o registro das ocorrências verificadas durante a execução contratual, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais e dando ciência ao gestor, conforme o caso.

11.2 - Há necessidade de adoção da penalidade de multa em quantitativos diversos daqueles estabelecidos no art. 160 da Portaria da CMBH nº 20.453/2022?
(X) Não.
( ) Sim. Da seguinte forma:

11.3 - Há necessidade de adoção de índice setorial específico para reajuste ?
( ) Não.
(X) Sim. O seguinte: Índice de Custo da Tecnologia da Informação (ICTI)

11.4 - Registrar a forma de recebimento do objeto e os prazos para sua aceitação provisória e definitiva: Vide itens 5.1.1 a 5.1.9 das CONDIÇÕES DE ACEITE E RECEBIMENTO deste ETP.".

12 - INFORMAÇÕES ADICIONAIS

A **forma de entrega dos bens** que compõem a solução deverá ser **única**.

O **prazo de entrega dos bens** que compõem a solução é de, no máximo, 60 (sessenta) dias corridos, a contar da data de emissão da ordem de compra pela CMBH.

A ativação do licenciamento e conclusão dos serviços de implantação e migração, deverão ocorrer em até 30 (trinta) dias corridos a contar da data de recebimento provisório pela CMBH dos bens que compõem a solução.

O início da prestação dos serviços de treinamento e operação assistida, deverá iniciar em até 5 (cinco) dias úteis a contar da data de conclusão dos serviços de implantação e respectivo aceite de conclusão desses pela CMBH, possuindo a duração de 10 (dez) dias úteis, conforme **"Subanexo C – Treinamento e operação**

assistida”.

O início da prestação dos serviços de suporte técnico e garantia, deverá ocorrer a partir da data de emissão da ordem de compra pela CMBH. Este serviço somente poderá ser faturado após o recebimento definitivo dos itens 1, 2 e 3. Só será considerado para fins de faturamento o período posterior à completa implantação e disponibilização da solução.

Os prazos de entrega poderão ser prorrogados somente mediante justificativa aceita pela CMBH.

13 - DATA E ASSINATURAS

Belo Horizonte, 30 de julho de 2024.

MEMBROS INTEGRANTES DA ELABORAÇÃO DO ETP:

COORDENADOR: Rafael Caetano Piva

Chefe da Seção de Infraestrutura de Tecnologia da Informação (SECITI) – CM 575

Servidores de Apoio:

RELATÓRIO DE ESTUDO TÉCNICO PRELIMINAR - ETP

Base legal: Lei Federal nº 14.133/2021

I - João Paulo Coelho Furtado
Analista de Tecnologia da Informação - CM 732

II - Fernando Cezar Pimenta
Analista de Tecnologia da Informação - CM 683

III - Pedro Paulo Martins da Fonseca
Chefe da Divisão de Tecnologia da Informação e Inovação - CM 576

ANEXO I - ESTIMATIVA DO VALOR DA CONTRATAÇÃO

(art. 18, §1º, inciso VI da Lei Federal nº 14.133/2021)

Seguem adiante as seguintes propostas comerciais e o detalhamento dos cálculos dos valores apresentados na tabela do item **4 - ESTIMATIVA DO VALOR DA CONTRATAÇÃO** para as três propostas:

- Proposta 1 - Cyberone
- Proposta 2 - Altasnet
- Proposta 3 - Actar

PROPOSTA TÉCNICA/COMERCIAL

REFRESH SOLUÇÂO NGFW PA3020
PALO ALTO NETWORKS

CÂMARA MUNIPAL DE BELO HORIZONTE

Contato CMBH: Lilian Oliveira
lillian.oliveira@cmbh.mg.gov.br

Contato Cyberone: Alessandra Brandão
alessandra.brandão@cyberone.com.br

DATA DE EMISSÃO: 14/12/2023

VALIDADE: 60 DIAS

SUMÁRIO

1. TERMO DE CONFIDENCIALIDADE 3
2. SOBRE A CYBERONE 4
3. OBJETIVO 5
3. CONTEÚDO DA PROPOSTA 5
4. COMUNICAÇÃO ENTRE AS PARTES 5
5. ESCOPO DA PROPOSTA 6
6. ARQUITETURA PALO ALTO NETWORKS 8
7. RELAÇÃO DE PARTNUMBERS ENVOLVIDOS 11
8. RESUMO DE INVESTIMENTO 14
9. CONDIÇÕES COMERCIAIS 17
10. ENCARGOS POR ATRASO DE PAGAMENTOS 18
11. METODOLOGIA DE EXECUÇÃO 19
12. ETAPAS DO PROJETO 19
12.1. PLANEJAMENTO 19
12.2. EXECUÇÃO 20
12.2.1. FASE 1 – ASSESSMENT 20
12.2.2. FASE 2 – INSTALAÇÃO, CONFIGURAÇÃO 20
12.2.3. FASE 3 – GO LIVE, OPERAÇÃO ASSISTIDA E HANDS-ON 20
12.2.4. FASE 4 – DOCUMENTAÇÃO DO PROJETO 21
12.2.5. FASE 4 – APRESENTAÇÃO DE RESULTADOS 21
12.3. ENCERRAMENTO 21
12.4. GERENCIAMENTO DO PROJETO 22
13. CRONOGRAMA MACRO DO PROJETO 22
14. PREMISSAS 23
15. ESTRUTURA ORGANIZACIONAL 24
18. EXPERTISE CYBERONE 28
19. TERMO DE ACEITE 39

1. TERMO DE CONFIDENCIALIDADE

Todas as informações contidas neste documento são consideradas CONFIDENCIAIS e destinam-se única e exclusivamente à análise da CONTRATANTE.

Por isso, ficam expressamente proibidas a reprodução e divulgação parcial ou total do conteúdo desta proposta, em mídia impressa ou eletrônica bem como informações contidas em materiais/conteúdos cedidos para o desenvolvimento do trabalho de consultoria.

O compartilhamento das informações supramencionadas poderá trazer vantagens significativas aos concorrentes da Cyberone, portanto, sua divulgação a funcionários da CONTRATANTE não envolvidos no processo, assim como a terceiros, é vetada, salvo com prévia autorização formal por parte da Cyberone.

Tanto a Contratante quanto a Cyberone se comprometem a manter sigilo em relação às informações confidenciais que tenham sido ou venham a ser reveladas ao longo do processo de negociação comercial e técnica.

O conteúdo desta proposta é de propriedade intelectual da Cyberone, não podendo ser reproduzido ou divulgado, exceto para fins de avaliação por parte de funcionários da Contratante. O acesso às informações contidas nas próximas páginas deste documento implica na concordância com os termos acima descritos.

A Cyberone agradece a oportunidade de apresentarmos os nossos serviços, e coloca-se à disposição para esclarecimentos adicionais sobre o exposto acima.

2. SOBRE A CYBERONE

Somos uma empresa com DNA mineiro, **Pure Player em Segurança da Informação**, com mais de 15 anos de experiência do nosso corpo diretivo, ótima parceira de negócios com expressivos casos de sucesso.

Nosso DNA é composto de ***INOVAÇÃO, EXPERTISE, LEALDADE, COMPROMISSO E PAIXÃO*** pelo que fazemos.

Contamos com time altamente capacitado, entregamos as melhores e mais inovadoras tecnologias do mercado, oferecemos serviços especializados de *Advisory* em Segurança da Informação, o que nos permite conhecer, entender e ofertar produtos e serviços que sempre irão agregar valor aos nossos parceiros de negócios.

Buscamos sempre apoiar e suportar nossos Clientes com soluções *premium* de segurança da informação bem como excelência nos serviços do pré ao pós-venda.

Com sede em Belo Horizonte e filial no Rio de Janeiro, atendemos de forma estruturada atuando e fidelizando o maior número de clientes durante nossa jornada.

A Cyberone possui diferenciais competitivos relevantes frente aos seus concorrentes o que nos permite entregar serviço na mais alta qualidade e valor agregado aos nossos clientes.

3. OBJETIVO

A presente proposta tem por objetivo fornecer a Câmara Municipal de Belo Horizonte solução de Next Generation Firewall PA 1410 com features de Advanced Threat Prevention, Advanced URL Filtering em cenário (AS-IS Atual) e opção de cenário (TO-BE Novas Funcionalidades) com novas features de Advanced Wildfire, DNS Security e Global Protect, com suporte Premium pelo período de 12 meses em substituição a solução atual PA3020, dentro das modalidades de fornecimento como Venda e Serviço.

3. CONTEÚDO DA PROPOSTA

O conteúdo dessa proposta destina-se exclusivamente à CONTRATANTE, não devendo ser divulgado fora de sua organização, nem duplicado, usado ou revelado, no todo ou em parte, para qualquer propósito que não seja o de avaliação do mesmo. Essa proposta foi baseada em informações retiradas do ambiente produtivo da CMBH. Quaisquer alterações destas implicarão na revisão das condições técnicas e comerciais propostas neste documento.

4. COMUNICAÇÃO ENTRE AS PARTES

Todas as informações transmitidas de uma parte a outra para validação do entendimento, para o aceite de documentos relacionados à prestação dos serviços propostos, sejam por meio eletrônico (email, FTP, Repositório Internet, etc.), ou meio físico (CD, Pendrive, Papel etc.), desde que passíveis de serem identificados o autor/publicador do conteúdo, terão validade legal para efeito de comunicação entre as partes.

5. ESCOPO DA PROPOSTA

O escopo dessa proposta contempla o fornecimento de solução de Next Generation Firewall PA 1410 contemplando o cenário atual com features de Advanced Threat Prevention, Advanced URL Filtering e cenário futuro com features de Advanced Wildfire, DNS Security e Global Protect, com suporte pelo período de 12 meses, dentro das modalidades de Venda e Serviço composta de:

- **Produto: Hardware, Suporte e Licenciamento PA1410 12 meses (OPÇÃO AS-IS VENDA)**

  - 02 x Palo Alto PA1410 Appliance
  - 02 x Power Cord BR
  - 02 x Advanced Threat Prevention em HA por 1 ano
  - 02 x Advanced URL Filtering em HA por 1 Ano
  - 02 x Premium Support por 1 ano

- **Produto: Hardware, Suporte e Licenciamento PA1410 12 meses (OPÇÃO AS-IS AS-A-SERVICE)**

  - 02 x Palo Alto PA1410 Appliance
  - 02 x Power Cord BR
  - 02 x Advanced Threat Prevention em HA por 1 ano
  - 02 x Advanced URL Filtering em HA por 1 Ano
  - 02 x Premium Support por 1 ano

- **Produto: Hardware, Suporte e Licenciamento PA1410 12 meses (OPÇÃO TO-BE VENDA)**

  - 02 x Palo Alto PA1410 Appliance
  - 02 x Power Cord BR
  - 02 x Bundle CoreSec (Advanced Threat Prevention, Advanced URL Filtering e Advanced Wildfire, DNS Security e SDWAN) em HA por 1 ano
  - 02 x Global Protect em HA por 1 Ano
  - 02 x Premium Support por 1 ano

- **Produto: Hardware, Suporte e Licenciamento PA1410 12 meses (OPÇÃO TO-BE AS-A-SERVICE)**

  - 02 x Palo Alto PA1410 Appliance
  - 02 x Power Cord BR
  - 02 x Bundle CoreSec (Advanced Threat Prevention, Advanced URL Filtering e Advanced Wildfire, DNS Security e SDWAN) em HA por 1 ano
  - 02 x Global Protect em HA por 1 Ano
  - 02 x Premium Support por 1 ano

- **Produto: Serviço de Instalação, Configuração, Migração, Operação Assistida e Hands-on**

  - 01 x Serviço de Instalação, Configuração, Migração, Operação Assistida e Hands-on

- **Produto: Serviço de Instalação Suporte e Manutenção 24x7 MSS 12 meses (CENÁRIO VENDA)**

  - 01 x Serviço de Suporte e Manutenção MSS 24x7 12 Meses

6. ARQUITETURA PALO ALTO NETWORKS

Features avançadas para NGFW:

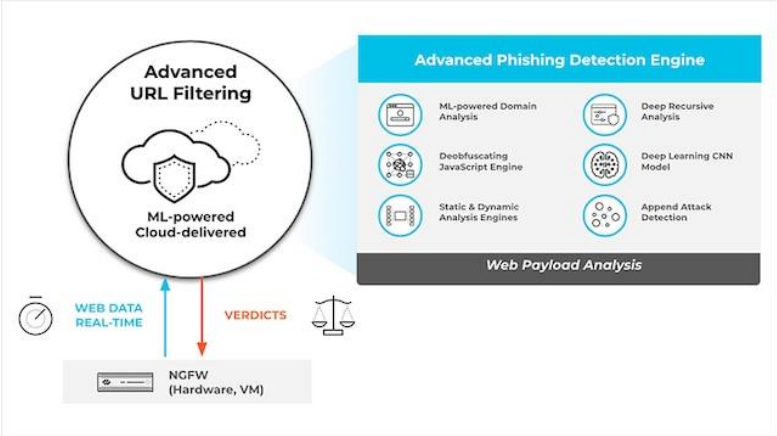
Os produtos abaixo da Palo Alto Networks fazem parte de um conjunto abrangente de soluções de segurança projetadas para proteger as organizações contra ameaças cibernéticas. Cada um deles desempenha um papel importante na defesa da rede, fornecendo recursos avançados de prevenção e detecção de ameaças.

Advanced Threat Prevention (Prevenção Avançada de Ameaças):

O Advanced Threat Prevention (ATP) é uma solução de segurança que utiliza várias técnicas avançadas para proteger contra ameaças cibernéticas. Ele combina recursos de prevenção de intrusões, sandboxing, análise comportamental e inteligência artificial para identificar e bloquear ameaças sofisticadas, como malware, ransomware e ataques direcionados. O ATP ajuda a proteger a rede contra ameaças conhecidas e desconhecidas, garantindo uma defesa proativa contra as mais recentes ameaças de segurança.

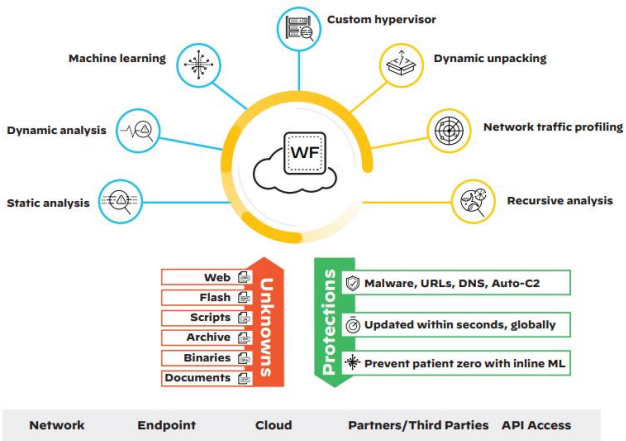
Advanced URL Filtering (Filtragem Avançada de URLs):

O Advanced URL Filtering é uma solução que fornece um controle granular sobre o acesso a sites e conteúdos na Internet. Ele permite que as organizações criem políticas de filtragem com base em categorias de sites, aplicando restrições ou permissões para garantir a conformidade com as políticas de segurança e conformidade da empresa. O URL Filtering ajuda a evitar o acesso a sites maliciosos, conteúdo impróprio ou não autorizado, protegendo a rede contra ameaças e mantendo a produtividade dos usuários.



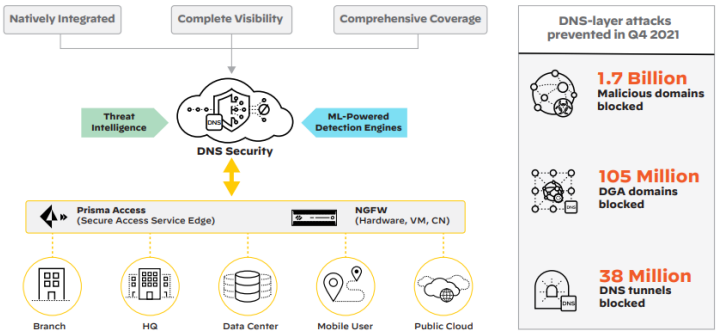
Advanced Wildfire (Wildfire Avançado):

O Advanced Wildfire é uma solução de sandboxing avançado que analisa arquivos e aplicativos desconhecidos em um ambiente isolado para identificar e bloquear ameaças avançadas. Ele usa técnicas de análise dinâmica, como execução em ambiente virtual, monitoramento de comportamento e detecção de malware em tempo real para identificar ameaças evasivas e de dia zero. O Wildfire Avançado ajuda a proteger a organização contra ameaças desconhecidas, enviando automaticamente informações sobre novas ameaças para a nuvem da Palo Alto Networks, para que sejam atualizadas as defesas em todas as instâncias do produto.



DNS Security (Segurança de DNS):

O DNS Security é uma solução que protege contra ameaças baseadas em DNS (Domain Name System). Ele monitora as solicitações de DNS em tempo real e utiliza análise comportamental e inteligência artificial para detectar e bloquear atividades maliciosas relacionadas a domínios, como comunicações com domínios de malware conhecidos, domínios de phishing e comunicações com domínios relacionados a ataques avançados. O DNS Security ajuda a prevenir ataques baseados em DNS e garante a segurança das comunicações online.



Global Protect (VPN):

O GlobalProtect da Palo Alto Networks é uma solução de segurança de rede líder no setor, projetada para proteger organizações em todo o mundo contra ameaças cibernéticas. Essa plataforma oferece uma variedade de recursos e funcionalidades essenciais para garantir a segurança de redes corporativas, independentemente de sua escala ou complexidade.

O GlobalProtect permite a criação de uma rede privada virtual (VPN) altamente segura, garantindo a conexão segura de funcionários, parceiros e dispositivos remotos à infraestrutura da empresa. Ele oferece autenticação multifator, criptografia avançada e políticas de segurança personalizáveis para proteger os dados e a integridade da rede.

Além disso, a solução fornece visibilidade abrangente e controle sobre o tráfego da rede, permitindo a detecção de ameaças em tempo real e a resposta rápida a incidentes de segurança. O GlobalProtect também é altamente escalável e se integra perfeitamente com outros produtos de segurança da Palo Alto Networks, tornando-o uma escolha confiável para organizações que buscam uma proteção abrangente contra ameaças cibernéticas.

7. RELAÇÃO DE PARTNUMBERS ENVOLVIDOS

Abaixo apresentamos a relação dos Partnumbers envolvidos no escopo dessa proposta:

Produto: PA1410 – Hardware, Licenciamento e Suporte 12 meses (AS-IS VENDA)

ITEM	DESCRIÇÃO	QTDE	TIPO
PA-PAN-PA-1410	Palo Alto Networks PA-1410	2	Hardware
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified	2	Hardware
PAN-PA-1410-ATP-HA2	PA-1410, Advanced Threat, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço
PAN-PA-1410-ADVURL-HA2	PA-1410, Advanced URL Filtering subscription, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.	2	Serviço

Produto: PA1410 – Hardware, Licenciamento e Suporte 12 meses (AS-IS AS-A-SERVICE)

ITEM	DESCRIÇÃO	QTDE	TIPO
PA-PAN-PA-1410	Palo Alto Networks PA-1410	2	Serviço
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified	2	Serviço
PAN-PA-1410-ATP-HA2	PA-1410, Advanced Threat, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço
PAN-PA-1410-ADVURL-HA2	PA-1410, Advanced URL Filtering subscription, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.	2	Serviço

Produto: PA1410 – Hardware, Licenciamento e Suporte 12 meses (TO-BE VENDA)

ITEM	DESCRIÇÃO	QTDE	TIPO
PA-PAN-PA-1410	Palo Alto Networks PA-1410	2	Hardware
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified	2	Hardware
PA-PAN-PA-3410-BND-CORESEC-1YR	PA-1410, Core Security Subscription Bundle (Advanced Threat Prevention, Advanced Url Filtering, Advanced Wildfire, Dns Security And Sd-Wan), 1 Year (12 Months) Term	2	Serviço
PAN-PA-1410-GP-HA2	PA-1410, GlobalProtect subscription, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.	2	Serviço

Produto: PA1410 – Hardware, Licenciamento e Suporte 12 meses (TO-BE AS-A-SERVICE)

ITEM	DESCRIÇÃO	QTDE	TIPO
PA-PAN-PA-1410	Palo Alto Networks PA-1410	2	Serviço
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified	2	Serviço
PA-PAN-PA-3410-BND-CORESEC-1YR	PA-1410, Core Security Subscription Bundle (Advanced Threat Prevention, Advanced Url Filtering, Advanced Wildfire, Dns Security And Sd-Wan), 1 Year (12 Months) Term	2	Serviço
PAN-PA-1410-GP-HA2	PA-1410, GlobalProtect subscription, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.	2	Serviço

Produto: Serviço de Instalação

ITEM	DESCRIÇÃO	QTDE	TIPO
CYBER-SRV01	Serviço de Instalação, Configuração, Migração, Operação Assistida e Hands-on	1	Serviço

Produto: Serviço de Suporte e Manutenção 24x7 MSS 12 meses (CENÁRIO VENDA)

ITEM	DESCRIÇÃO	QTDE	TIPO
CYBER-SRV01	Serviço de Suporte e Manutenção 24x7 MSS 12 Meses	1	Serviço

8. RESUMO DE INVESTIMENTO

Produto: HARDWARE, LICENCIAMENTO E SUPORTE PA 1410 (AS-IS VENDA)

ITEM	DESCRIÇÃO	QTDE	TIPO	VALOR
CMBH HARDWARE, LICENÇAS E SUPORTE PA1410 AS-IS VENDA				
PA-PAN-PA-1410	Palo Alto Networks PA-1410	2	Hardware	**R$ 404.882,37**
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified	2	Hardware	
PAN-PA-1410-ATP-HA2	PA-1410, Advanced Threat, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço	
PAN-PA-1410-ADVURL-HA2	PA-1410, Advanced URL Filtering subscription, for one (1) device in an HA pair, 1 year (12 months) term.	2	Serviço	
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.	2	Serviço	
TOTAL				**R$ 404.882,37**

Produto: HARDWARE, LICENCIAMENTO E SUPORTE PA 1410 (AS-IS AS-A-SERVICE)

ITEM	DESCRIÇÃO	QTDE	TIPO	VALOR MÊS
CMBH HARDWARE, LICENÇAS E SUPORTE PA1410 AS-IS AS-A-SERVICE				
PA-PAN-PA-1410	Palo Alto Networks PA-1410	12	Serviço	**R$ 50.252,90**
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified			
PAN-PA-1410-ATP-HA2	PA-1410, Advanced Threat, for one (1) device in an HA pair, 1 year (12 months) term.			
PAN-PA-1410-ADVURL-HA2	PA-1410, Advanced URL Filtering subscription, for one (1) device in an HA pair, 1 year (12 months) term.			
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.			
TOTAL				**R$ 603.034,80**

Produto: HARDWARE, LICENCIAMENTO E SUPORTE PA 1410 (TO-BE VENDA)

ITEM	DESCRIÇÃO	QTDE	TIPO	VALOR MÊS
CMBH HARDWARE, LICENÇAS E SUPORTE PA1410 TO-BE VENDA				
PA-PAN-PA-1410	Palo Alto Networks PA-1410	2	Hardware	**R$ 497.166,63**
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified	2	Hardware	
PAN-PA-1410-BND-CORESEC	PA-1410 Core Security Subscription Bundle Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security and SD-WAN 1 years 12 months term	2	Serviço	
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.	2	Serviço	
TOTAL				**R$ 497.166,63**

Produto: HARDWARE, LICENCIAMENTO E SUPORTE PA 1410 (TO-BE AS-A-SERVICE)

ITEM	DESCRIÇÃO	QTDE	TIPO	VALOR MÊS
CMBH HARDWARE, LICENÇAS E SUPORTE PA1410 TO-BE AS-A-SERVICE				
PA-PAN-PA-1410	Palo Alto Networks PA-1410	12	Serviço	**R$ 58.797,28**
PAN-PWR-C19-BR	Power Cord, Brazil, 16A, 250V, NBR14136 (IEC 60906-1) to IEC-60320-C19, 10-FT, Brazilian INMETRO certified			
PAN-PA-1410-BND-CORESEC	PA-1410 Core Security Subscription Bundle Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security and SD-WAN 1 years 12 months term			
PAN-SVC-PREM-1410	PA-1410, Premium support, 1 year (12 months) term.			
TOTAL				**R$ 705.567,35**

Produto: SERVIÇO DE INSTALAÇÃO (CENÁRIO VENDA)

ITEM	DESCRIÇÃO	QTDE	TIPO	VALOR
CMBH – SERVIÇO DE INSTALAÇÃO				
CYBER-SRV01	Serviço de Instalação, Configuração, Migração, Operação Assistida e Hands-on	1	Serviço	**R$ 18.000,00**
TOTAL				**R$ 18.000,00**

Produto: SERVIÇO DE SUPORTE 24x7 MSS 12 MESES (CENÁRIO VENDA)

ITEM	DESCRIÇÃO	QTDE	TIPO	VALOR MÊS
SOTREQ – SERVIÇO DE ACOMPANHAMENTO SERVIDORES				
CYBER-SRV01	Serviço de Suporte e Manutenção 24x7 MSS 12 meses	12	Serviço	**R$7.200,00**
TOTAL				**R$86.400,00**

9. CONDIÇÕES COMERCIAIS

Hardware, Softwares e Licenças

- ✓ Prazo de Pagamento: 30 dias corridos após emissão da nota fiscal;
- ✓ Valor final a ser convertido onde será considerado a conversão do dólar de acordo com o valor da PTAX do dia anterior na emissão das ordens de compra, que a CONTRATANTE terá o prazo máximo de 10 dias para a sua emissão após o valor definitivo da PTAX;
- ✓ Valores sujeitos à alteração após vencimento da proposta e/ou alteração de tabela do fabricante;
- ✓ Licenças serão enviadas por e-mail;
- ✓ Previsão de Entrega HW: 90 dias corridos após a confirmação do pedido;
- ✓ Atrasos na fabricação/disponibilização poderão afetar o prazo de entrega;
- ✓ Garantia: Prazo e as condições de garantia são de responsabilidade do Fabricante;
- ✓ A emissão do faturamento ocorrerá por meio da Cyberone Tecnologia e Segurança da Informação Ltda | CNP:10.303.057/0001-13 | IE: 003765678.00-50
- ✓ Sujeito a análise e crédito e/ou alteração por filiais;
- ✓ O presente contrato não permite cancelamento ou desistência dos itens deste anexo por qualquer motivo que seja (incluindo questões ligadas à variação do dólar, às licenças adquiridas e a fatos ligados ao respectivo Fabricante), de modo que a CONTRATANTE deverá adquirir e pagar a integralidade das licenças descritas no Anexo, durante o período previsto neste instrumento.
- ✓ Inclusos despesas de viagem, alimentação e transporte;

10. ENCARGOS POR ATRASO DE PAGAMENTOS

Em caso de impontualidade do cliente em efetuar qualquer pagamento a seu cargo, haverá incidência automática de correção monetária positiva pelo IGPM/FGV (ou índice que venha a substituí-lo), juros de mora à razão de 1% (um por cento) ao mês (calculados pro -rata die), bem como multa moratória por parcela em atraso à razão de 10% (dez por cento) incidente no 5º dia contado do vencimento. Esses encargos decorrentes da mora incidirão sobre o saldo devedor atualizado até sua efetiva quitação.

Havendo necessidade de cobrança judicial de débitos serão devidos honorários advocatícios à razão de 20% (vinte por cento) do valor total da dívida.

O cliente declara-se ciente e autoriza que a falta de pagamento de qualquer obrigação implicará protesto dos respectivos títulos e a informação da inadimplência a órgãos de proteção ao crédito, tais como SERASA e SPC, entre outros.

11. METODOLOGIA DE EXECUÇÃO

O Projeto será executado de acordo com a metodologia de Gerenciamento de Projetos da Cyberone que é que está aderente às práticas descritas no PMBOK – Project Management Body of Knowledge publicado pelo PMI (Project Management Institute).

12. ETAPAS DO PROJETO

12.1. PLANEJAMENTO

Nesta etapa são realizadas as atividades de planejamento do projeto, bem como as entregas serão especificadas e o cronograma detalhado é elaborado em atendimento:

- aos objetivos e requisitos do projeto;
- às expectativas do cliente;
- ao orçamento do projeto.

Atividades

- Realizar reunião inicial de planejamento;
- Detalhar cronograma do projeto;
- Elaborar Relatório de Planejamento do Projeto;
- Realizar reunião de kick-off;
- Ajustar e disponibilizar o planejamento;
- Aprovar planejamento do projeto.

Produtos da etapa

- Cronograma detalhado;
- Relatório de Planejamento do Projeto;
- Apresentação em pdf utilizada na reunião de kick-off.

12.2. EXECUÇÃO

As fases detalhadas abaixo fazem parte do escopo de serviços solicitado na RFP.

12.2.1. FASE 1 – Assessment

Nessa etapa será realizada a análise e avaliação da arquitetura proposta compreendendo as seguintes atividades:

- Análise das Configurações de Rede implementadas;
- Análise das Configurações atuais dos NGFWs PA 3020 implementados;
- Definição da Topologia;
- Confecção do HLD;

12.2.2. FASE 2 – Instalação, Configuração

Nessa etapa será realizada a instalação, configuração da solução Palo Alto PA1410 a ser executado pelo técnico local da CONTRATADA em Belo Horizonte, acompanhado pela CONTRATANTE, conforme atividades abaixo:

- Instalação física no rack da localidade;
- Inserção da interface de gerência na rede local;
- Ativação de licenças e novas features de segurança;
- Realização do Backup de Configuração (XML) da solução de NGFWs atual PA3020;
- Inserção do Backup XML nos novos appliances PA1410;
- **Necessária a disponibilidade de recurso da contratada.**

12.2.3. FASE 3 – Go Live, Operação Assistida e Hands-on

Nessa etapa será realizada a ativação da solução Palo Alto Networks em ambiente produtivo, bem como o processo de passagem de conhecimento hands-on e operação assistida conforme atividades abaixo:

- Elaboração e Apresentação do Plano de Migração
- Realização de testes de alta disponibilidade dos clusters, durante a janela de migração;
- Virada de ambiente e validação das configurações (regras de firewall, objetos de firewall, entre outros);
- Operação Assistida (in loco) pós-virada de até 2 dias.
- Realização da coleta de dados;
- **Atividade realizada com equipe presencial e remota no Datacenter**

12.2.4. FASE 4 – DOCUMENTAÇÃO DO PROJETO

Nessa etapa será elaborada toda a documentação do Projeto (as built) contendo no mínimo as seguintes informações:

- Apresentação do documento
- Cenário implementado
- Topologia da rede
- Solução de firewall
- Configurações
- Performance
- Relatório Palo Alto BPA (Best Practice Assessment)

12.2.5. FASE 4 – APRESENTAÇÃO DE RESULTADOS

Nesta etapa será realizada uma reunião onde serão apresentados de forma executiva os resultados do projeto.

Produtos da etapa:

- Apresentação em pdf dos resultados do projeto.

12.3. ENCERRAMENTO

Nesta etapa serão realizadas as atividades de encerramento do projeto, como:

- Verificação se a entregas realizadas correspondem ao que foi contratado;
- Fechamento do controle financeiro do projeto;
- Desmobilização da equipe do projeto;
- Obtenção do termo de aceite final do projeto e do atestado de capacidade técnica na execução do projeto.

Produtos da etapa:

- Termo de aceite final do projeto.
- Atestado de capacidade técnica.

12.4. GERENCIAMENTO DO PROJETO

Esta etapa permeia todas as demais etapas do projeto. É nela que serão realizadas as atividades de gestão do projeto, incluindo o controle financeiro, identificação e tratamento dos riscos, reuniões de alinhamento com a equipe interna e reuniões de status com a equipe da Câmara Municipal de Belo Horizonte para apresentar a evolução do projeto, alinhar expectativas, verificar pendências e definir ações para mitigação de riscos, validação das entregas realizadas e apresentação executiva de resultados do projeto.

Produtos da etapa:

- Apresentação em pdf do status do projeto;
- Atas das reuniões de status.

13. CRONOGRAMA MACRO DO PROJETO

O cronograma abaixo demonstra de forma macro como serão executadas as fases do projeto, estipuladas com datas fictícias estimadas;

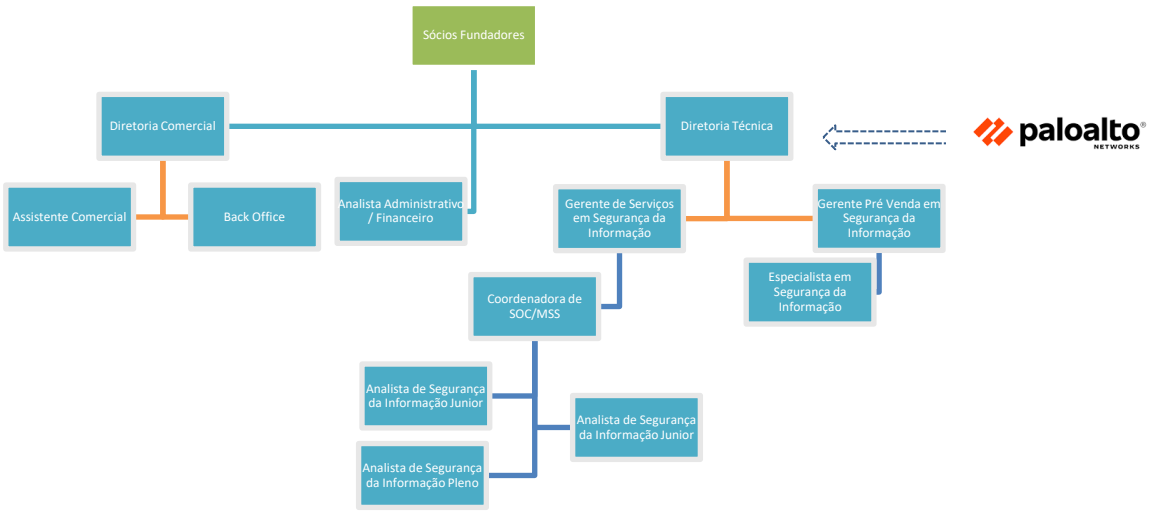
Task Name	Duration Days	Start	Finish
Projeto Palo Alto Networks - Substituição PA3020	**122**	**01/06/2024**	**-**
1.Comercial	**93**	01/06/2024	02/09/2024
1.1.Formalização do Pedido	3	01/06/2024	04/06/2024
1.2.Assinatura do Contrato	15	01/06/2024	16/06/2024
1.3.Entrega do Equipamentos	90	01/06/2024	30/08/2024
2.Planejamento do Projeto	**5**	01/06/2024	06/06/2024
2.1.Elaboração do Plano de Projeto	5	01/06/2024	06/06/2024
2.2.Matriz de Risco	5	01/06/2024	06/06/2024
2.3.Conograma Detalhado	5	01/06/2024	06/06/2024
2.4.Renião de Kick Off	1	01/06/2024	02/06/2024
2.5.Aprovação do Plano de Projeto	5	01/06/2024	06/06/2024
3.Execução	**22**	30/08/2024	21/09/2024
3.1.FASE 1 - Assessment	5	07/06/2024	12/06/2024
3.2.FASE 2 - Instalação e Configuração	5	30/08/2024	04/09/2024
3.3.FASE 3 - Go Live, Operação Assistida e Hands-on	2	05/09/2024	07/09/2024
3.4.FASE 4 - Documentação	10	07/09/2024	17/09/2024
4.Encerramento	**2**	18/09/2024	20/09/2024
4.1.Apresentação de Resultados	1	21/09/2024	22/09/2024
4.2.Termo de Aceite e Atestado de Capacidade	1	23/09/2024	24/09/2024
FIM		**-**	**24/09/2024**

14. PREMISSAS

- A CONTRATADA só realizará tarefas que estejam dentro do escopo definido por esse documento. Quaisquer mudanças no escopo do projeto deverão ser aprovadas pela CONTRATADA e pela CONTRATANTE reavaliando, caso necessário, as condições comerciais;
- Os serviços serão realizados em modalidade hibrida, parte presencial e parte remota;
- A CONTRATANTE deverá alocar a quantidade de profissionais necessários para a execução do projeto de modo a não comprometer os prazos estabelecidos.
- A CONTRATANTE deverá fornecer a documentação da topologia de rede, endereços IPs e demais configurações do ambiente atual;
- A CONTRATANTE deverá fornecer acesso à CONTRATADA aos equipamentos do ambiente atuais para realização do Assessment;
- Qualquer necessidade de viagem fora do município de Belo Horizonte, os custos relacionados serão de responsabilidades da CONTRATANTE.
- A CONTRATADA não é a responsável pela correção das vulnerabilidades encontradas durante a execução do Projeto;
- A CONTRATADA não é responsável pela operação e ajustes de demais equipamentos que não sejam os detalhados nessa proposta.
- O que não estiver explicitamente incluso no escopo discriminado ao longo deste documento, premissas e restrições da proposta, está implicitamente excluso.
- O serviço de suporte e manutenção 24x7 MSS contempla a utilização de 37 horas mês não acumulativas.

15. ESTRUTURA ORGANIZACIONAL

Abaixo apresentamos a Estrutura Organizacional da Cyberone que estará envolvida no Projeto da Câmara Municipal de Belo Horizonte:



16.

Nome	Cargo	Email	Telefone
Renata Melo	Diretora Comercial	renata@cybeorne.com.br	(31) 98104-8772
Fernando Freitas	Diretor Técnico	fernando@cybeorne.com.br	(31) 99939-7469
Nelson Charret	Gerente de Serviços em Segurança da Informação	nelson.charret@cyberone.com.br	(31) 3653.5501
Jorge Souza	Gerente de Pré Venda em Segurança da Informação	jorge.souza@cyberone.com.br	(31) 3653.5501
Isabela Rabello	Coordenadora de SOC/MSS	isabela.rabello@cyberone.com.br	(31) 3653.5501
Renan Henrique	Especialista em Segurança da Informação	renan.henrique@cyberone.com.br	(31) 3653.5501
Lucas Mariano	Analista de Segurança da Informação Junior	lucas.mariano@cyberone.com.br	(31) 3653.5501
Alan Santos	Analista de Segurança da Informação Junior	alan.santos@cyberone.com.br	(31) 3653.5501
Gustavo Telles	Analista de Segurança da Informação Pleno	gustavo.telles@cyberone.com.br	(31) 3653.5501

MINI CURRICULO	
Fernando Freitas	Sócio Fundador e Diretor Técnico da Cyberone Profissional com mais de 20 anos de experiência no mercado de Segurança da Informação, tendo atuado como Consultor de Segurança por mais de 11 anos. Foi CISO do Banco Olé Consignado e CSO do Banco BS2. Já liderou projetos de segurança em diversas empresas dos mais diversos segmentos. Liderou projeto de Gestão de Riscos de Segurança da Informação no BPC da Angola. Possui MBA em Gerenciamento de Projetos pela FGV e as certificações CDPSE, ISO Leader Auditor 27001, MCSO, CobiT
Nelson Charret	Profissional de TI a mais de 24 anos, nos últimos 10 anos atuando na área de segurança da informação, focando em entregar projetos contendo as melhores soluções de segurança do mercado. Especializado em soluções da Palo Alto, F5 e Cisco. Já executou inúmeros projetos contendo implementações de soluções de segurança em redes de grande escala e alta complexidade, aos quais destacamos CEMIG, SOTREQ, PETROS e LIGHT. Possui as certificações **PCNSE (Palo Alto Certified System Engieneer)**, ICSI | CNSS Certified Network Security Specialist, ITIL V3, COBIT 4.1
Jorge Souza	Especialista em Segurança da Informação com mais de 20 anos de experiência no setor. Histórico sólido em empresas líderes do segmento como Trend Micro e Forcepoint, com ênfase em projetos de segurança cibernética. **Certificado PMP/PMI** o que complementa a sua habilidade em liderar projetos de alta complexidade fornecendo soluções personalizadas de Data Protection, Endpoint Protection, Data Loss Prevention e Network Security para diversos **clientes no Brasil e América Latina.**"

MINI CURRICULO	
Isabela Rabello	Atuante na área de Segurança da Informação há 7 anos, com foco em implantação, operação e suporte de firewalls CheckPoint e WatchGuard e suas blades de segurança para alguns clientes como MRS Logística, Tribunal de Justiça do Estado do Rio de Janeiro, PUC Minas, WeWork, entre outros. Possui as certificações **AWS CCP (Certified Cloud Practitioner), CheckPoint CCSA, CheckPoint CCSE** e curso completo CCME (CheckPoint Certified Maestro Expert) para implantação de ambientes escaláveis.
Renan Henrique	Profissional de TI a mais de 16 anos, nos últimos 13 anos atuando na área de telecomunicações com ênfase em segurança da informação, focando em entregar projetos de conectividade e infraestrutura diversos como 5G, WIFI, IoT, SDN, MPLS, Clouds, contemplando as melhores soluções de segurança do mercado. Especializado em soluções da Huawei, Cisco, Dell, Infinera, Fortinet e Claroty e também em Backup Seguro com soluções Dell e Commvault. Já executou inúmeros projetos contendo implementações de soluções de segurança em redes de grande escala e alta complexidade com protocolos LAN, WAN, SDN, GPON e MPLS, aos quais destacamos CEMIG, MRS Logística. Possui grande expressividade no mercado de Telecomunicações para ambientes OT/IT onde já palestrou sobre os temas em eventos Nacionais e Internacionais como o Huawei Connect em Xangai. Entre as certificações da Palo Alto destacamos abaixo: **Palo Alto Networks Systems Engineer (PSE): Cortex Associate, Prisma Cloud Associate, Prisma SASE Associate, Strata Associate, Software Firewall Associate e Palo Alto Networks Systems Engineer (PSE): Strata Professional.**

MINI CURRICULO	
Lucas Mariano	Analista de Segurança da Informação, atua como suporte técnico de sistemas e equipamentos de segurança da informação níveis I e II, monitoramento, análise e resposta a incidentes, desenvolvendo e aplicando segurança e inteligência ao negócio com regras de segurança customizadas ao ambiente. **Possui certificação CISCO CCNA, e Palo Alto Networks Systems Engineer (PSE): Strata Professional.**
Alan Santos	Analista de Segurança da Informação, atua como suporte técnico de sistemas e equipamentos de segurança da informação níveis I e II, monitoramento, análise e resposta a incidentes, desenvolvendo e aplicando segurança e inteligência ao negócio com regras de segurança customizadas ao ambiente.
Gustavo Telles	Analista de Segurança da Informação, atua como suporte técnico de sistemas e equipamentos de segurança da informação níveis I e II, monitoramento, análise e resposta a incidentes, desenvolvendo e aplicando segurança e inteligência ao negócio com regras de segurança customizadas ao ambiente. **Possui a certificação PCNSA (Palo Alto Certified System Administrator) da Palo Alto Neworks**

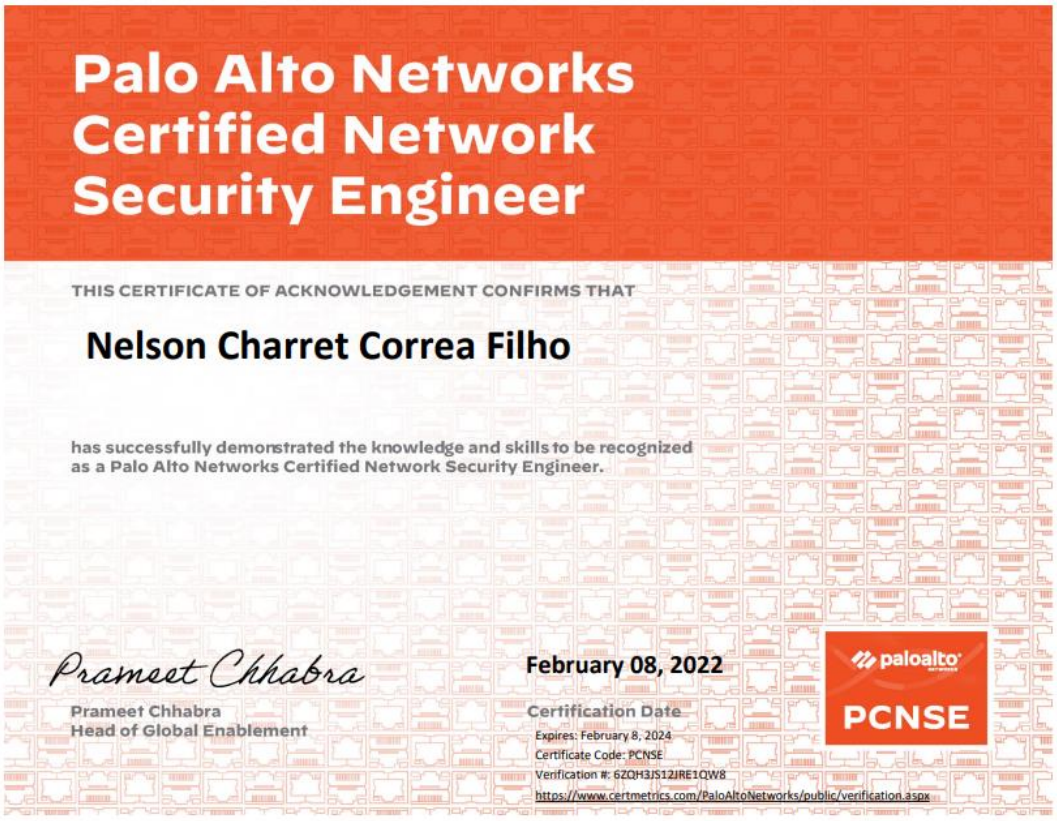
18. EXPERTISE CYBERONE

A Cyberone conta com profissionais altamente capacitados e experientes no que se refere a Segurança da Informação, tendo participado de diversos projetos semelhantes ao da Câmara Municipal de Belo Horizonte, aos quais destacamos:

- CEMIG: Projeto de Venda e Implementação de 02 (dois) clusters da solução Palo Alto Networks PA-5220 nos ambientes COS (Centro de Operação do Sistema) e COD (Centro de Operações da Distribuição) com as funcionalidades de Threat Prevention.
- CEMIG: Projeto de Venda e Implementação de 47 (quarente e sete) equipamentos da Solução Palo Alto PA-220R com as funcionalidades de Threat Prevention e Panorama, em subestações de energia da CEMIG pelo Estado de Minas Gerais.
- SAMARCO: Projeto de Venda e Implementação de 04 (oito firewalls) clusters PA 440 com as funcionalidades de Threat Prevention e WildFire para proteção do ambiente de Automação na Unidade de Mariana.
- Banco INTER: Projeto de Venda e Implementação da solução Palo Alto Networks PA-3220;
- UFJF (Universidade Federal de Juiz de Fora): Projeto de Venda e Implementação da solução Palo Alto Networks PA-3250.
- PUC-MG (Pontifícia Universidade Católica de Minas Gerais): Projeto de Suporte da solução Palo Alto modelo PA-3220, cluster, com as funcionalidades de Threat Prevention, URL Filtering, Virtual Systems e Panorama em um ambiente de 60.000 (sessenta mil) usuários.
- BANCO BS2: Venda e Implementação de solução Palo Alto Networks em ambiente híbrido (on Premise e Cloud), com as funcionalidades de Threat Prevention e URL Filtering para um ambiente de 1.000 (mil) usuários.
- BANCO BMG: Venda de licenciamento e operação MSS de toda a solução de NGFW Palo Alto Networks PA 3220 envolvendo serviços críticos de Call Center e PIX.

Abaixo alguns de nossos principais clientes:

CERTIFICAÇÕES E CAPACIDADE TÉCNICA:



Palo Alto Networks
Certified Network
Security Engineer

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

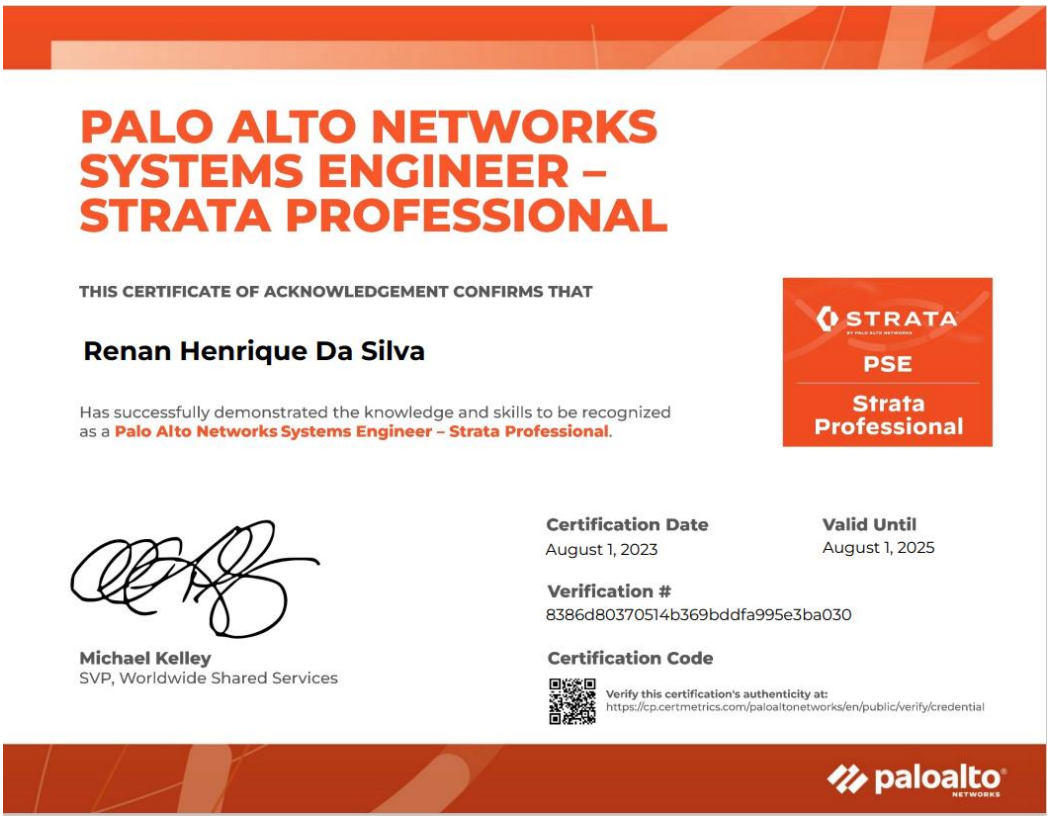
Nelson Charret Correa Filho

has successfully demonstrated the knowledge and skills to be recognized as a Palo Alto Networks Certified Network Security Engineer.

Prameet Chhabra
Prameet Chhabra
Head of Global Enablement

February 08, 2022
Certification Date
Expires: February 8, 2024
Certificate Code: PCNSE
Verification #: 6ZQH3JS12JRE1QW8
https://www.certmetrics.com/PaloAltoNetworks/public/verification.aspx

paloalto
PCNSE



PALO ALTO NETWORKS
SYSTEMS ENGINEER –
STRATA PROFESSIONAL

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Renan Henrique Da Silva

Has successfully demonstrated the knowledge and skills to be recognized as a **Palo Alto Networks Systems Engineer – Strata Professional**.

STRATA
PSE
Strata Professional

Michael Kelley
SVP, Worldwide Shared Services

Certification Date
August 1, 2023

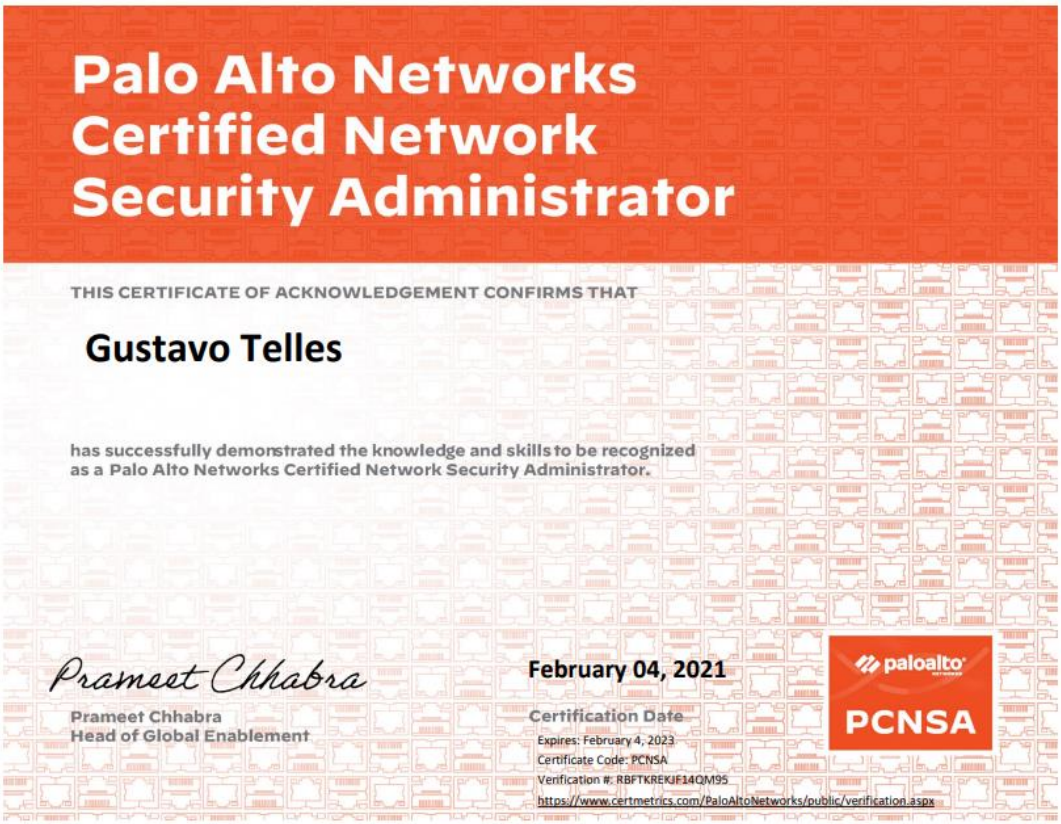
Valid Until
August 1, 2025

Verification #
8386d80370514b369bddfa995e3ba030

Certification Code

Verify this certification's authenticity at:
https://cp.certmetrics.com/paloaltonetworks/en/public/verify/credential

paloalto



Palo Alto Networks
Certified Network
Security Administrator

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Gustavo Telles

has successfully demonstrated the knowledge and skills to be recognized as a Palo Alto Networks Certified Network Security Administrator.

Prameet Chhabra
Prameet Chhabra
Head of Global Enablement

February 04, 2021
Certification Date

Expires: February 4, 2023
Certificate Code: PCNSA
Verification #: RBFTKREKJF14QM95
https://www.certmetrics.com/PaloAltoNetworks/public/verification.aspx

paloalto
PCNSA

paloalto NETWORKS

Certificate of Completion

This is to certify that

Fernando Freitas

has successfully completed

Palo Alto Networks Accredited Systems Engineer (PSE): Strata Associate Accreditation Exam

Date: *9/24/2020*

Prameet Chhabra
Prameet Chharbra
Head of Global Enablement

CDPSE Certified Data Privacy Solutions Engineer
An ISACA® Certification

ISACA hereby certifies that

Fernando Freitas

has successfully met all requirements and is qualified as a Certified Data Privacy Solutions Engineer; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include meeting the eligibility requirements for professional experience; adherence to the ISACA Code of Professional Ethics and the CDPSE continuing professional education policy.

2112491	15 February 2021	31 January 2025
Certificate Number	Date of Certification	Expiration Date

ISACA

ISACA Chief Executive Officer

ATESTADO DE CAPACIDADE TÉCNICA

A empresa Banco BS2 S.A, empresa privada com sede na Avenida Raja Gabaglia, 1143 – 14º ao 16º andar - Luxemburgo, Belo Horizonte – MG, inscrita no CNPJ sob o no 71.027.866/0001-34 , atesta para os devidos fins que a empresa Cyberone Tecnologia e Segurança da Informação Ltda, inscrita no CNPJ sob o no 10.303.057/0001-13, situada na Rua Antônio de Albuquerque, 330 – Sala 901 – Funcionários, Belo Horizonte – MG, realizou o serviços de Comercialização, Instalação, Configuração e Suporte da solução de firewall Palo Alto Networks existente no ambiente Datacenter Local e ambiente Nuvem (Cloud) contemplando um total de 1.000 usuários conforme relação abaixo:

- Cluster Palo Alto Networks VM-300 ambiente Cloud
- Cluster Palo Alto Networks PA 5020 ambiente Onpremise
- Palo Alto Networks Threat Prevention
- Palo Alto Networks URL FIltering
- Palo Alto Networks Panorama Central Management
- Palo Alto Networks Premium Support

Atestamos que os serviços foram executados de forma satisfatória e dentro dos prazos estabelecidos, não havendo até a presente data, nada em nossos arquivos que desabonem a empresa Cyberone Tecnologia e Segurança da Informação Ltda, referente a sua conduta e responsabilidade no que fiz respeito à venda, prazo de entrega, assistência técnica/comercial e obrigações assumidas dos serviços acima citados.

Belo Horizonte, 09 de novembro de 2020

71.027.866/0001-34
BANCO BS2 S/A
AV. Raja Gabaglia, nº 1.143
14º ao 16º andar
Luxemburgo - CEP: 30.380-403
BELO HORIZONTE - MG

Eli de Souza e Silva Júnior
Coordenador de TI
(31) 3078-8115
eli.junior@bs2tecnologia.com.br

brembo do brasil

Atestamos para os devidos fins, que a empresa **CYBERONE TECNOLOGIA E SEGURANCA DA INFORMACAO LTDA**, CNPJ 10.303.057/0001-13, localizada à Rua Queluzita, nº 34 sala 605 bloco 02, Bairro Dom Joaquim, Belo Horizonte - MG, realizou os serviços de Comercialização e Treinamento Técnico da solução de Next Generation Firewall Palo Alto Networks conforme descrito abaixo:

- 02 x Equipamentos Palo Alto Networks PA 820 em Alta Disponibilidade;
- 12 x conectores SFP Transceiver 100Base-T;
- 02 x Licenças da funcionalidade Threat Prevention em alta disponibilidade;
- 02 x Licenças da funcionalidade URL Filtering em alta disponibilidade;
- Suporte e Garantia Oficial do fabricante para os 02 equipamentos.

Atestamos que os serviços foram executados de forma satisfatória e dentro dos prazos estabelecidos, não havendo até a presente data, nada em nossos arquivos que desabonem a empresa Cyberone Tecnologia e Segurança da Informação Ltda, referente a sua conduta e responsabilidade no que fiz respeito à venda, prazo de entrega, assistência técnica/comercial e obrigações assumidas dos serviços acima citados.

Betim, 28 de janeiro de 2022
Nome do Responsável: Cristiano Luiz Gomes de Freitas
Cargo: IT MANAGER
Telefone: +55 31 3539.8578
Email: cristiano.freitas@brembodobrasil.com.br

BREMBO DO BRASIL Ltda Betim Plant
www.brembo.com
Av. Fausto Ribeiro da Silva, 1.265
Distrito Industrial Bandeirinhas - CEP 32654-805
Betim -MG - Brasil
Fone: +55 31 3539 8500 - Fax: +55 31 3539 8511
CNPJ 03.645.767/0001-66

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE JUIZ DE FORA
COORDENADORIA DE SUPRIMENTOS

CERTIDÃO

Anna Cecília Assis Mendonça – Coordenadora de Suprimentos da Universidade Federal de Juiz de Fora, no exercício de seu cargo e na forma lei, etc.

Certifica a pedido da interessada e para fins de participação em licitação pública, que a empresa **CYBERONE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO LTDA**, com sede na Rua Antônio de Albuquerque nº 330 – Sala 901 - Savassi, na cidade de Belo Horizonte - MG, inscrita no CNPJ sob o número 10.303.057/00001-13, forneceu para a Universidade Federal de Juiz de Fora, 01 (UN) SOLUÇÃO DE PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE "NEXT GENERATION FIREWALL - NGFW" PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL QUE INCLUI FIREWALL, CONTROLE DE APLICAÇÃO, ADMINISTRAÇÃO DE LARGURA DE BANDA (QOS), SUPORTE PARA CONEXÕES VPN IPSEC E SSL, IPS, PREVENÇÃO CONTRA AMEAÇAS DE VÍRUS, SPYWARES E MALWARES , FILTRO DE URL, BEM COMO CONTROLE DE TRANSMISSÃO DE DADOS E ACESSO A INTERNET; COMPOSTA POR 2 (DUAS) UNIDADES DO TIPO APPLIANCE PARA FUNCIONAMENTO EM MODELO ATIVO- PASSIVO COM CAPACIDADE DE GERAÇÃO E CUSTOMIZAÇÃO DE RELATÓRIOS TÉCNICOS E GERENCIAIS COM BASE NAS INFORMAÇÕES DE SEGURANÇA GERADAS PELO SISTEMA. LICENCIAMENTO, SUPORTE E GARANTIA PARA O PERÍODO DE 1 ANO. Marca: PANW-FIREWALL NGFW-Modelo: PA 3250, relativo à Licitação PR 0078/2020, dentro dos prazos e condições estabelecidos nos procedimentos licitatórios. Certifica ainda, que a referida documentação encontra-se em seu poder e arquivo. Certifica e dá fé.x.x.x

SMC SOCIEDADE MINEIRA de CULTURA | Gerência de Tecnologia da Informação

Belo Horizonte, 03 de novembro de 2020

ATESTADO DE CAPACIDADE TÉCNICA

A empresa Sociedade Mineira de Cultura - PUC Minas, com sede na Avenida Francisco Sales, nº 540 - Floresta, Belo Horizonte - MG, inscrita no CNPJ sob o no 17.178.195/0025-34 , atesta para os devidos fins que a empresa Cyberone Tecnologia e Segurança da Informação Ltda, inscrita no CNPJ sob o no 10.303.057/0001-13, situada na Rua Antônio de Albuquerque, nº 330 - Sala 901 - Savassi, Belo Horizonte - MG, realiza os serviços de Configuração e Suporte Técnico da solução de firewall do tipo Next Generation da fabricante Palo Alto Networks existente no ambiente Datacenter Local contemplando um total de 60.000 usuários conforme relação abaixo:

- Cluster Palo Alto Networks PA 3220
- Palo Alto Networks Threat Prevention
- Palo Alto Networks URL Filtering
- Palo Alto Networks Virtual Systems
- Palo Alto Networks Panorama Central Management

Atestamos que os serviços são executados de forma satisfatória e dentro dos prazos estabelecidos, não havendo, até a presente data, nada em nossos arquivos que desabonem a empresa Cyberone Tecnologia e Segurança da Informação Ltda, referente à sua conduta e responsabilidade no que diz respeito às obrigações assumidas para os serviços acima citados.

Marcelo Nassau Malta
Gerente de Tecnologia da Informação
smcgti@pucminas.br
(31) 3249.7301

SMC/Gerência de Tecnologia da Informação
Av. Francisco Sales, 540 – 2º andar - Floresta - 30150-220 - Belo Horizonte - MG
(31) 3249.7300 - Fax (31) 3249-7323

SAMARCO

Atestamos para os devidos fins, que a empresa **CYBERONE TECNOLOGIA E SEGURANCA DA INFORMACAO LTDA**, CNPJ 10.303.057/0001-13, localizada à Rua Queluzita, nº 34 sala 605 bloco 02, Bairro Dom Joaquim, Belo Horizonte - MG, realizou os serviços de Comercialização, Instalação, Configuração e Treinamento Técnico da solução de Next Generation Firewall Palo Alto Networks conforme descrito abaixo:

- 08 x Equipamentos Palo Alto Networks PA 440 em Alta Disponibilidade (04 clusters);
- 08 x Licenças da funcionalidade Threat Prevention em alta disponibilidade;
- 08 x Licenças da funcionalidade WildFire em alta disponibilidade;
- Suporte e Garantia Oficial do fabricante para os 08 equipamentos;
- Serviços de Instalação, Configuração, Migração e Operação Assistida;
- 02 x Vouchers de Treinamento Oficial da Palo Alto Networks PAN 210 – Firewall – Essentials – Configuration and Management

Atestamos que os serviços foram executados de forma satisfatória e dentro dos prazos estabelecidos, não havendo até a presente data, nada em nossos arquivos que desabonem a empresa Cyberone Tecnologia e Segurança da Informação Ltda, referente a sua conduta e responsabilidade no que fiz respeito à venda, prazo de entrega, assistência técnica/comercial e obrigações assumidas dos serviços acima citados.

Mariana, 09 de fevereiro de 2023
Nome do Responsável: Alexandre Carvalho Martins
Cargo: Gerência de Engenharia de Processos e Automação
Telefone: +55 31 3559.5440
Email: acmartins@samarco.com

Clicksign

Datas e horários em GMT -03:00 Brasilia
Log gerado em 09 de fevereiro de 2023. Versão v1.20.0.

Atestado de Capacidade Técnica_Palo Alto_Samarco.pdf

Documento número #2b9fd6c9-9c63-44cd-8765-ce33cc756871
Hash do documento original (SHA256): 5e142cc050340a28d9d79734880262d6f16073d088027ea0bce93e9058bf2128

Assinaturas

Alexandre Carvalho Martins
CPF: 047.041.966-07
Assinou como contratante em 09 fev 2023 às 16:01:22

Log

09 fev 2023, 14:13:40	Operador com email financeiro@cyberone.com.br na Conta 64b6b942-9138-455e-9b67-58013b3dba66 criou este documento número 2b9fd6c9-9c63-44cd-8765-ce33cc756871. Data limite para assinatura do documento: 10 de fevereiro de 2023 (14:12). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
09 fev 2023, 14:13:40	Operador com email financeiro@cyberone.com.br na Conta 64b6b942-9138-455e-9b67-58013b3dba66 adicionou à Lista de Assinatura: acmartins@samarco.com para assinar como contratante, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Alexandre Carvalho Martins e CPF 047.041.966-07.
09 fev 2023, 16:01:22	Alexandre Carvalho Martins assinou como contratante. Pontos de autenticação: Token via E-mail acmartins@samarco.com. CPF informado: 047.041.966-07. IP: 201.48.224.194. Componente de assinatura versão 1.443.0 disponibilizado em https://app.clicksign.com.
09 fev 2023, 16:01:23	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 2b9fd6c9-9c63-44cd-8765-ce33cc756871.

ICP Brasil

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://validador.clicksign.com e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 2b9fd6c9-9c63-44cd-8765-ce33cc756871, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

19. TERMO DE ACEITE

Informamos que estamos de acordo com o descrito nesta proposta e firmamos o nosso aceite.

Partes envolvidas:

CONTRATANTE	**CONTRATADA**
NOME:	**NOME:** Cyberone Tecnologia e Segurança da Informação
CNPJ:	**CNPJF:** 10.303.057/0001-13
IE:	**IE:** 003765678.00-50
ENDEREÇO:	**ENDEREÇO:** Rua Queluzita, 34 – Sala 605 Bloco 2 B. Dom Joaquim, BH/MG

Representantes Legais das partes envolvidas:

CONTRATANTE	CONTRATADA
Nome:	Nome:
CPF:	CPF:

TESTEMUNHAS:

1._____	1._____
Nome:	Nome:
CPF:	CPF:

Altasnet

Proposta Comercial – Nº 2554_24

FORNECIMENTO DE CLUSTER DE FIREWALL

CMBH

CÂMARA MUNICIPAL DE BELO HORIZONTE

AVISO DE CONFIDENCIALIDADE

A informação contida em todas as páginas deste documento/proposta é confidencial da Altasnet. Ao receber o documento, o destinatário concorda em manter tais informações em sigilo e não reproduzir ou divulgar a qualquer pessoa fora do grupo diretamente responsável pela avaliação do conteúdo, a menos que a Altasnet tenha autorizado. Portanto, este documento é apenas para fins informativos devendo ser considerado para os negócios da Altasnet. A Altasnet nem seus representantes serão responsáveis sobre qualquer ato do destinatário ou de seus representantes, como resultado do uso das informações aqui fornecidas. A assinatura de um acordo definitivo ou assinatura de aceitação da proposta, por representantes autorizados das partes, será o único meio pelo qual a Altasnet ou suas afiliadas serão vinculadas à proposta/contrato.

ESCLARECIMENTO

Dúvidas ou esclarecimentos sobre esta Política de Privacidade, entre em contato com seu representante de vendas.

INFORMAÇÕES SOBRE ESTE DOCUMENTO

Histórico de Versões

Versão	Data	Autor/Revisor	Descrição
01	14/12/2023	Lissandro Santos	Proposta Comercial

Histórico de revisões desta Proposta Comercial.

Recursos envolvidos

Função | Responsável

Função	Responsável
Gerente de Contas	**Lissandro Santos** Executivo de Vendas (31) 98799-6976 lissandro@altasnet.com.br
Assistente Comercial	**Weverton Diniz** Weverton.soares@altasnet.com.br

APRESENTAÇÃO INSTITUCIONAL

A Altasnet é uma empresa líder do mercado na prestação de serviços e soluções da área de Tecnologia da Informação (TI), capaz de suprir e apoiar o crescimento das organizações.

Nós entendemos que as inovações tecnológicas impulsionam o mercado e exigem mudanças dentro das empresas, já que estão transformando como nos relacionamos e trabalhamos. Quem aderir às novas ferramentas desenvolverá vantagens competitivas e oportunidades no mundo dos negócios.

Nossa equipe e portfólio suprem essas necessidades, fornecendo consultoria para a análise de cenários e implantação de produtos até o gerenciamento de soluções. A confiança dos parceiros depositada em nosso trabalho está refletida nos números da Altasnet:

PRODUTOS

Gerenciar uma infraestrutura de TI não depende exclusivamente de uma única solução, mas de um conjunto de ferramentas e softwares para gerar eficiência e segurança.

Com experiência há mais de 21 anos, a Altasnet disponibiliza diversas soluções, divididas em cinco grupos:

Inovação

Ajuste rapidamente a escala de suas operações de serviço de atendimento ao consumidor e de TI. A ServiceNow permite fluxos de trabalho digitais para estimular o crescimento dos negócios, aumentar a resiliência e aprimorar a produtividade dos funcionários

Redes

Projetamos e implementamos redes locais com recursos consistentes para Data Centers, Redes Corporativas, Campus e Filiais. Os desenhos das soluções oferecem alto desempenho, capacidade de expansão e ampla gama de recursos de conectividade. Contamos com um portfólio completo de ativos de rede, rico em recursos com foco em alto desempenho, segurança e gerência para atender empresas de pequeno, médio e grande porte.

Segurança

Disponibilizamos um conjunto de soluções de segurança em tempo real, fornecendo segurança proativa de antivírus baseado em IA, firewall, IPS, anti-spam, filtros de conteúdo e gerenciamento da internet.

Data Center

A consolidação de servidores e virtualização é uma das principais alternativas para otimização dos recursos de TI, gerando alta disponibilidade dos serviços e redução drástica de custos. Nossos sistemas de armazenamento de dados contemplam soluções de Storage NAS (Network Attached Storage), SAN (Storage Area Network) e backup de fabricantes líderes de mercado.

Serviços

Fornecemos diversas ferramentas para auxiliar no gerenciamento e acompanhar todos os serviços de TI de uma empresa com o objetivo de melhorar a produtividade dos colaboradores por meio de respostas proativas em tempo real.

Para implantá-las, a Altasnet conta com especialistas em integrar recursos tecnológicos com potencial disruptivo, para proporcionar a modernização, transformação e inovação.

Somos preparados para resolver questões complexas de tecnologia, nossas soluções são customizadas para atender as especificidades dos clientes, levando o que precisam para a melhoria do seu ambiente físico e virtual.

PAPÉIS E RESPONSABILIDADES

A **CMBH.** deverá fiscalizar a execução dos serviços, bem como:

- Propiciar todas as facilidades necessárias à boa execução deste serviço, inclusive comunicando à Altasnet, por escrito e tempestivamente, qualquer mudança de administração e endereço de cobrança;
- Permitir ao pessoal técnico da Altasnet acesso (físico e lógico) aos equipamentos que serão utilizados no serviço desta proposta, e, as dependências onde serão apresentados, testados e instalados os mesmos. Respeitadas as normas que disciplinam a segurança do patrimônio, das pessoas e das informações;
- Receber os serviços/produtos testá-los e, quando atenderem ao objeto da proposta, aprová-los.

A **CMBH.** compromete-se em ceder os profissionais e recursos necessários à correta definição e prestação do serviço contratado. Para tanto necessitaremos do apoio das áreas responsáveis pela infraestrutura de informática da empresa.

É necessário que a **CMBH.** forneça as mídias de instalação de todos os softwares envolvidos em eventuais instalações, além dos recursos de hardware e infraestrutura de rede necessária para a execução dos serviços.

É de responsabilidade da **CMBH.** manter cópia (backup) garantida e segura de todas as informações que porventura estejam em seus servidores e sejam relacionadas diretamente ou indiretamente com a prestação do serviço; por exemplo, arquivos e bancos de dados, e outros documentos do projeto.

Caso sejam necessárias quaisquer interrupções no ambiente de produção do usuário, a informação, análise de impacto, negociação do tempo de parada e demais formalizações devem ser realizadas pela **CMBH.**

DA ALTASNET

A empresa Altasnet deverá efetuar os serviços dentro do prazo proposto, bem como:

- Responsabilizar-se por todos e quaisquer acidentes que venham a ser vítimas os seus empregados quando em serviço, por tudo quanto as leis trabalhistas e previdenciárias lhes assegurem e demais exigências legais para o exercício da atividade;
- Sujeitar-se a fiscalização por parte do Cliente, prestando-lhe todos os esclarecimentos solicitados e atendendo às reclamações formuladas;
- Assumir todos e quaisquer ônus referentes a salário, horas extras, outros adicionais e demais encargos sociais, referentes aos seus empregados.
- Manter sigilo sobre qualquer informação obtida durante os trabalhos.

A Altasnet não é responsável por:

- Perda de dados ou informações decorrentes de defeitos de hardware e software (bugs) ou por qualquer operação realizada no ambiente sem a indicação da Altasnet;
- Customizações no ambiente ou instalação de produtos que não os pertinentes ao escopo do serviço. A Altasnet só realizara customizações necessárias à prestação dos serviços descritos no escopo desta proposta;
- Conceder especial prioridade para os serviços ora contratados, salvo por motivo de força maior, devidamente comprovado, não podendo transferi-los a outrem, no todo ou em parte, sem prévia e expressa concordância do Cliente;
- Realizar readequações no ambiente para execução dos serviços contratados. Caso a readequação seja necessária será cobrado do cliente a sua execução em projeto a parte.

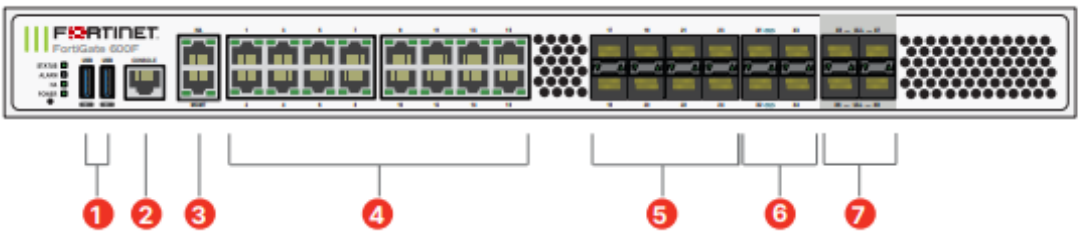
A Altasnet apoiará o cliente nas análises e definições técnicas especificamente necessárias ao escopo do trabalho

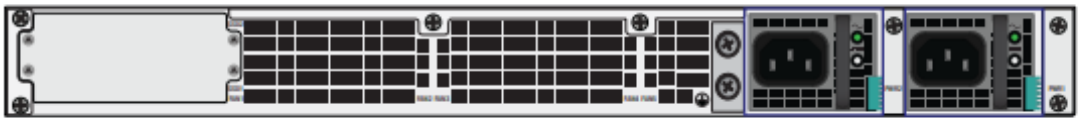
DESCRITIVO TÉCNICO

CLUSTER DE FIREWALL FORTINET MODELO: FG600F

Hardware

FortiGate 600F Series

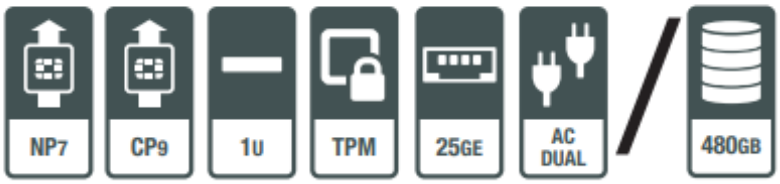




Interfaces

1. 2 x USB Ports
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Slots
5. 8 x GE SFP Slots
6. 4 x 10GE/GE SFP+/SFP Slots
7. 4x 25GE/10GE SFP28/ SFP+ Ultra Low Latency Slots

Hardware Features



FORTIAUTHENTICATOR VM LICENCIADO PARA 300 USUÁRIOS

Specifications

VIRTUAL APPLIANCES	FAC-VM BASE	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG
Capacity				
Users (Local and Remote)	100	+100	+1000	+10 000
FortiTokens	200	+200	+2000	+20 000
NAS Devices	33	+33	+333	+3333
User Groups	10	+10	+100	+1000
CA Certificates	5	+5	+50	+500
User Certificates	500	+500	+5000	+50 000
Virtual Machine				
Hypervisors Supported	VMware ESXi/ ESX 6/ 7/ 8, Microsoft Hyper-V Server 2010, 2012 R2, 2016, and 2019, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV (Acropolis Hypervisor), Oracle OCI, Alibaba Cloud			
Maximum Virtual CPUs Supported	64			
Virtual NICs Required (Minimum / Maximum)	1 / 4			
Virtual Machine Storage (Minimum / Maximum)	60 GB / 16 TB			
Virtual Machine Memory Required (Minimum / Maximum)	2 GB / 1 TB			
High Availability Support	Active-Passive HA and Config Sync HA			

CONDIÇÕES COMERCIAIS

ITEM	DESCRIÇÃO	TIPO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	**APPLIANCE FORTIGATE MODELO FG600F**	HARDWARE	2	R$ 257.840,00	R$ 515.680,00
1.1	**LICENCIAMENTO PARA FIREWALL FG600F PARA 3 ANOS** Licenciamento Unified Threat Protection (UTP) para Firewall FG600F (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) Para 36 Meses	SOFTWARE	2	R$ 342.570,00	R$ 685.140,00
2	**LICENCIAMENTO BASE FORTIAUTHENTICATOR VM PARA 300 USUARIOS INCLUINDO SUPORTE E GARANTIA DO FABRICANTE PARA 3 ANOS** VM Base License supports 100 users. Manager and QEMU 2.5.0, and Xen Virtual Machine platforms Upgrade FortiAuthenticator-VM 200 users license upgrade FortiAuthenticator	SOFTWARE	1	R$ 41.591,00	R$ 41.591,00
3	Serviço técnico especializado de instalação e configuração e repasse de conhecimento do Firewall e FortiAuthenticator durante o horário comercial	SERVIÇO	1	R$ 26.880,00	R$ 26.880,00
4	Suporte técnico especializado durante 36 meses	SERVIÇO	36	R$ 2.080,00	R$ 74.880,00
VALOR TOTAL					**R$ 1.344.171,00**

Validade da Proposta

Os preços são válidos até **14/02/2024**

Altas Networks e Telecom Ltda
CNPJ: 05.407.609/0001-01
Representante Mandatário – Lissandro Flávio dos Santos

05.407.609/0001-01
I.E: 062.212.833.0032
Altas Networks e Telecom Ltda.
Rua Juruá, 46 - 7º Andar - Salas 704 a 708
Bairro da Graça – CEP: 31140-020
BELO HORIZONTE – MG

Altasnet

Proposta Comercial – Nº 2554_24

LOCAÇÃO DE CLUSTER DE FIREWALL

CMBH

CÂMARA MUNICIPAL DE BELO HORIZONTE

AVISO DE CONFIDENCIALIDADE

A informação contida em todas as páginas deste documento/proposta é confidencial da Altasnet. Ao receber o documento, o destinatário concorda em manter tais informações em sigilo e não reproduzir ou divulgar a qualquer pessoa fora do grupo diretamente responsável pela avaliação do conteúdo, a menos que a Altasnet tenha autorizado. Portanto, este documento é apenas para fins informativos devendo ser considerado para os negócios da Altasnet. A Altasnet nem seus representantes serão responsáveis sobre qualquer ato do destinatário ou de seus representantes, como resultado do uso das informações aqui fornecidas. A assinatura de um acordo definitivo ou assinatura de aceitação da proposta, por representantes autorizados das partes, será o único meio pelo qual a Altasnet ou suas afiliadas serão vinculadas à proposta/contrato.

ESCLARECIMENTO

Dúvidas ou esclarecimentos sobre esta Política de Privacidade, entre em contato com seu representante de vendas.

INFORMAÇÕES SOBRE ESTE DOCUMENTO

Histórico de Versões

Versão	Data	Autor/Revisor	Descrição
01	14/12/2023	Lissandro Santos	Proposta Comercial

Histórico de revisões desta Proposta Comercial.

Recursos envolvidos

Função | Responsável

Função	Responsável
Gerente de Contas	**Lissandro Santos** Executivo de Vendas (31) 98799-6976 lissandro@altasnet.com.br
Assistente Comercial	**Weverton Diniz** Weverton.soares@altasnet.com.br

APRESENTAÇÃO INSTITUCIONAL

A Altasnet é uma empresa líder do mercado na prestação de serviços e soluções da área de Tecnologia da Informação (TI), capaz de suprir e apoiar o crescimento das organizações.

Nós entendemos que as inovações tecnológicas impulsionam o mercado e exigem mudanças dentro das empresas, já que estão transformando como nos relacionamos e trabalhamos. Quem aderir às novas ferramentas desenvolverá vantagens competitivas e oportunidades no mundo dos negócios.

Nossa equipe e portfólio suprem essas necessidades, fornecendo consultoria para a análise de cenários e implantação de produtos até o gerenciamento de soluções. A confiança dos parceiros depositada em nosso trabalho está refletida nos números da Altasnet:

PRODUTOS

Gerenciar uma infraestrutura de TI não depende exclusivamente de uma única solução, mas de um conjunto de ferramentas e softwares para gerar eficiência e segurança.

Com experiência há mais de 21 anos, a Altasnet disponibiliza diversas soluções, divididas em cinco grupos:

Inovação

Ajuste rapidamente a escala de suas operações de serviço de atendimento ao consumidor e de TI. A ServiceNow permite fluxos de trabalho digitais para estimular o crescimento dos negócios, aumentar a resiliência e aprimorar a produtividade dos funcionários

Redes

Projetamos e implementamos redes locais com recursos consistentes para Data Centers, Redes Corporativas, Campus e Filiais. Os desenhos das soluções oferecem alto desempenho, capacidade de expansão e ampla gama de recursos de conectividade. Contamos com um portfólio completo de ativos de rede, rico em recursos com foco em alto desempenho, segurança e gerência para atender empresas de pequeno, médio e grande porte.

Segurança

Disponibilizamos um conjunto de soluções de segurança em tempo real, fornecendo segurança proativa de antivírus baseado em IA, firewall, IPS, anti-spam, filtros de conteúdo e gerenciamento da internet.

Data Center

A consolidação de servidores e virtualização é uma das principais alternativas para otimização dos recursos de TI, gerando alta disponibilidade dos serviços e redução drástica de custos. Nossos sistemas de armazenamento de dados contemplam soluções de Storage NAS (Network Attached Storage), SAN (Storage Area Network) e backup de fabricantes líderes de mercado.

Serviços

Fornecemos diversas ferramentas para auxiliar no gerenciamento e acompanhar todos os serviços de TI de uma empresa com o objetivo de melhorar a produtividade dos colaboradores por meio de respostas proativas em tempo real.

Para implantá-las, a Altasnet conta com especialistas em integrar recursos tecnológicos com potencial disruptivo, para proporcionar a modernização, transformação e inovação.

Somos preparados para resolver questões complexas de tecnologia, nossas soluções são customizadas para atender as especificidades dos clientes, levando o que precisam para a melhoria do seu ambiente físico e virtual.

PAPÉIS E RESPONSABILIDADES

A **CMBH.** deverá fiscalizar a execução dos serviços, bem como:

- Propiciar todas as facilidades necessárias à boa execução deste serviço, inclusive comunicando à Altasnet, por escrito e tempestivamente, qualquer mudança de administração e endereço de cobrança;
- Permitir ao pessoal técnico da Altasnet acesso (físico e lógico) aos equipamentos que serão utilizados no serviço desta proposta, e, as dependências onde serão apresentados, testados e instalados os mesmos. Respeitadas as normas que disciplinam a segurança do patrimônio, das pessoas e das informações;
- Receber os serviços/produtos testá-los e, quando atenderem ao objeto da proposta, aprová-los.

A **CMBH.** compromete-se em ceder os profissionais e recursos necessários à correta definição e prestação do serviço contratado. Para tanto necessitaremos do apoio das áreas responsáveis pela infraestrutura de informática da empresa.

É necessário que a **CMBH.** forneça as mídias de instalação de todos os softwares envolvidos em eventuais instalações, além dos recursos de hardware e infraestrutura de rede necessária para a execução dos serviços.

É de responsabilidade da **CMBH.** manter cópia (backup) garantida e segura de todas as informações que porventura estejam em seus servidores e sejam relacionadas diretamente ou indiretamente com a prestação do serviço; por exemplo, arquivos e bancos de dados, e outros documentos do projeto.

Caso sejam necessárias quaisquer interrupções no ambiente de produção do usuário, a informação, análise de impacto, negociação do tempo de parada e demais formalizações devem ser realizadas pela **CMBH.**

DA ALTASNET

A empresa Altasnet deverá efetuar os serviços dentro do prazo proposto, bem como:

- Responsabilizar-se por todos e quaisquer acidentes que venham a ser vítimas os seus empregados quando em serviço, por tudo quanto as leis trabalhistas e previdenciárias lhes assegurem e demais exigências legais para o exercício da atividade;
- Sujeitar-se a fiscalização por parte do Cliente, prestando-lhe todos os esclarecimentos solicitados e atendendo às reclamações formuladas;
- Assumir todos e quaisquer ônus referentes a salário, horas extras, outros adicionais e demais encargos sociais, referentes aos seus empregados.
- Manter sigilo sobre qualquer informação obtida durante os trabalhos.

A Altasnet não é responsável por:

- Perda de dados ou informações decorrentes de defeitos de hardware e software (bugs) ou por qualquer operação realizada no ambiente sem a indicação da Altasnet;
- Customizações no ambiente ou instalação de produtos que não os pertinentes ao escopo do serviço. A Altasnet só realizara customizações necessárias à prestação dos serviços descritos no escopo desta proposta;
- Conceder especial prioridade para os serviços ora contratados, salvo por motivo de força maior, devidamente comprovado, não podendo transferi-los a outrem, no todo ou em parte, sem prévia e expressa concordância do Cliente;
- Realizar readequações no ambiente para execução dos serviços contratados. Caso a readequação seja necessária será cobrado do cliente a sua execução em projeto a parte.

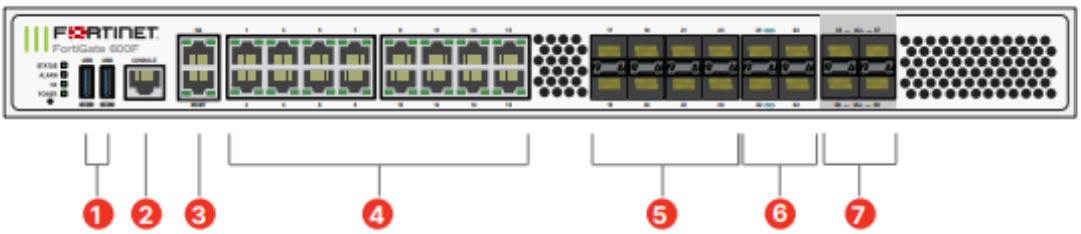
A Altasnet apoiará o cliente nas análises e definições técnicas especificamente necessárias ao escopo do trabalho

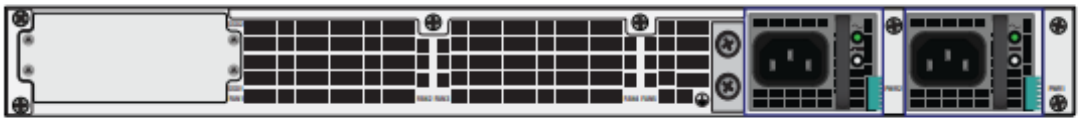
DESCRITIVO TÉCNICO

CLUSTER DE FIREWALL FORTINET MODELO: FG600F

Hardware

FortiGate 600F Series

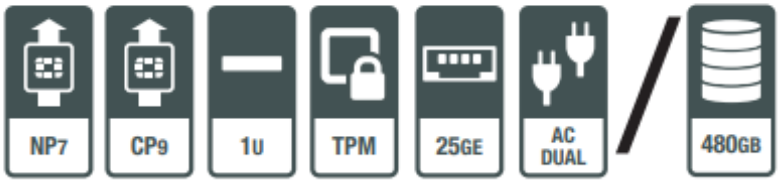




Interfaces

1. 2 x USB Ports
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Slots
5. 8 x GE SFP Slots
6. 4 x 10GE/GE SFP+/SFP Slots
7. 4x 25GE/10GE SFP28/ SFP+ Ultra Low Latency Slots

Hardware Features



FORTIAUTHENTICATOR VM LICENCIADO PARA 300 USUÁRIOS

Specifications

VIRTUAL APPLIANCES	FAC-VM BASE	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG
Capacity				
Users (Local and Remote)	100	+100	+1000	+10 000
FortiTokens	200	+200	+2000	+20 000
NAS Devices	33	+33	+333	+3333
User Groups	10	+10	+100	+1000
CA Certificates	5	+5	+50	+500
User Certificates	500	+500	+5000	+50 000
Virtual Machine				
Hypervisors Supported	VMware ESXi/ ESX 6/ 7/ 8, Microsoft Hyper-V Server 2010, 2012 R2, 2016, and 2019, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV (Acropolis Hypervisor), Oracle OCI, Alibaba Cloud			
Maximum Virtual CPUs Supported	64			
Virtual NICs Required (Minimum / Maximum)	1 / 4			
Virtual Machine Storage (Minimum / Maximum)	60 GB / 16 TB			
Virtual Machine Memory Required (Minimum / Maximum)	2 GB / 1 TB			
High Availability Support	Active-Passive HA and Config Sync HA			

CONDIÇÕES COMERCIAIS - OPEX

ITEM	DESCRIÇÃO	TIPO	VALOR MENSAL UNITÁRIO PARA 36 MESES
1	**APPLIANCE FORTIGATE MODELO FG600F**	HARDWARE	**R$ 19.812,00**
1.1	**LICENCIAMENTO PARA FIREWALL FG600F PARA 3 ANOS** Licenciamento Unified Threat Protection (UTP) para Firewall FG600F (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) Para 36 Meses	SOFTWARE	**R$ 25.517,00**
2	**LICENCIAMENTO BASE FORTIAUTHENTICATOR VM PARA 300 USUARIOS INCLUINDO SUPORTE E GARANTIA DO FABRICANTE PARA 3 ANOS** VM Base License supports 100 users. Manager and QEMU 2.5.0, and Xen Virtual Machine platforms Upgrade FortiAuthenticator-VM 200 users license upgrade FortiAuthenticator	SOFTWARE	**R$ 1.925,00**
3	Serviço técnico especializado de instalação e configuração e repasse de conhecimento do Firewall e FortiAuthenticator durante o horário comercial	SERVIÇO	**R$ 1.022,00**
4	Suporte técnico especializado durante 36 meses	SERVIÇO	**R$ 2.080,00**
VALOR TOTAL			**R$ 50.356,00**

Validade da Proposta

Os preços são válidos até **14/02/2024**

Altas Networks e Telecom Ltda
CNPJ: 05.407.609/0001-01
Representante Mandatário – Lissandro Flávio dos Santos

05.407.609/0001-01
I.E: 062.212.833.0032
Altas Networks e Telecom Ltda.
Rua Juruá, 46 - 7º Andar - Salas 704 a 708
Bairro da Graça – CEP: 31140-020
BELO HORIZONTE – MG

Belo Horizonte, 26 de dezembro de 2023.

Para
CMBH
A.C.: Erica Ceciane
E-mail: erika.ceciane@cmbh.mg.gov.br

Proposta: ACT23-BH-16546 -R00

REF.: Fornecimento de solução Check Point Quantum com serviços de configuração inicial e suporte técnico ACTAR.

1. APRESENTAÇÃO

A ACTAR fornece soluções completas e serviços especializados em CyberSecurity. Visando atender este mercado de forma qualificada, a ACTAR coloca à disposição de sua empresa, profissionais certificados nas diversas tecnologias desenvolvidas por fabricantes líderes de mercado, a saber: ***CheckPoint, Illumio, VU, OX, Aqua Security, Vicarius, Cybereason, Radware, Cymulet, Tenable, Securi.AI, SecuPI, Juniper Networks e Cisco Systems, entre outras***.

Estamos certos de que a proposta encaminhada por nós será uma oportunidade de um efetivo trabalho em conjunto com a equipe da CMBH.

Através de nosso know-how e parceria com os maiores fabricantes podemos proporcionar à sua equipe e à sua empresa serviços diferenciados, facilitando a administração de sua Network, sua Cyber Security e sua Cloud.

2. OBJETIVO

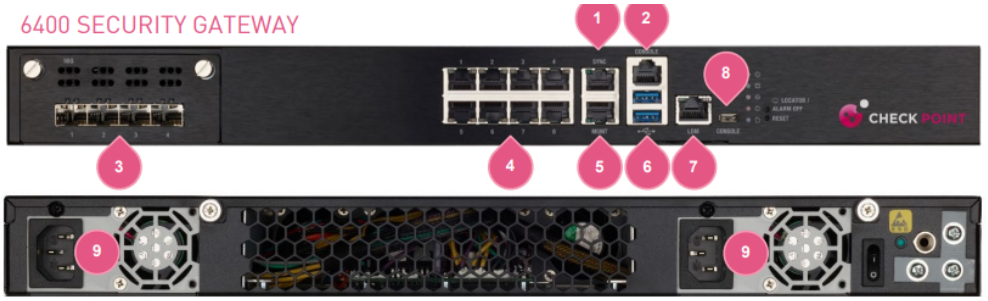
O objetivo desta proposta é o fornecimento de solução Check Point Quantum com serviços ACTAR de configuração inicial e suporte técnico 24x7.

3. SOLUÇÃO CHECK POINT QUANTUM

FIREWALLS DE PRÓXIMA GERAÇÃO - NGFW

Os gateways da Check Point oferecem segurança superior além de qualquer Firewall de Próxima Geração (NGFW). Melhor projetados para a proteção Zero Day da SandBlast, esses gateways são os melhores na prevenção da quinta geração de ataques cibernéticos com mais de 60 serviços de segurança inovadores. Baseada na Infinity Architecture, a nova linha Quantum Security Gateway™ de 15 modelos pode oferecer até 1,5 Tbps de desempenho de prevenção de ameaças e pode ser dimensionada sob demanda.

CHECK POINT QUANTUM 6400 SECURITY GATEWAY



1. Sync 10/100/1000 Base-T port	6. 2x USB 3.0 ports
2. RJ45 console port	7. Lights-out Management port
3. 1 network expansion slot	8. USB Type-C console port
4. 8x 10/100/1000 Base-T ports	9. Redundant power supplies
5. Management 10/100/1000 Base-T port	

Proteger empresas de médio porte com até 5000 funcionários requer uma solução de segurança escalável que expanda as proteções contra ataques cibernéticos GenV enquanto o negócio cresce. A série Quantum Security Gateway ™ 6000 expande rapidamente o desempenho de prevenção de ameaças da SandBlast Network, começando com até 7,6 Gbps com expansão de hiperescala de até 380 Gbps. Aproveitando o gerenciamento unificado do Infinity, as empresas podem reduzir as operações de segurança em até 80%.

Com prevenção de dia zero pronta para uso, a família Quantum 6000 protege contra ataques GenV com prevenção de ameaças de até 7,6 Gbps. Com o Maestro Hyperscale, a prevenção de ameaças pode ser expandida até 380 Gbps em apenas alguns minutos. A resiliência no nível da nuvem é fornecida com 100% SSDs e fontes de alimentação redundantes. A conectividade 2 x 40 GbE é fornecida para redes em rápido crescimento. O gerenciamento unificado oferece flexibilidade por meio dos serviços de nuvem de segurança SmartConsole ou SmartCloud no local.

Segurança inflexível

Oferece prevenção contra ameaças de alto calibre com a premiada proteção SandBlast Zero Day pronta para uso.

Segurança em hiperescala

Desempenho de prevenção de ameaças em hiperescala sob demanda, fornecendo às empresas expansão do nível de nuvem e resiliência no local

Segurança unificada

O controle de gerenciamento de segurança unificado R81 em redes, nuvens e IoT aumenta a eficiência, reduzindo as operações de segurança em até 80%

Integrando o mais avançado em prevenção contra ameaças e gerenciamento consolidado, nossos gateways de segurança foram criados para evitar qualquer ataque cibernético, reduzir a complexidade e diminuir seus custos.

actar
PEERS group

Serviço de segurança de rede

Amplie facilmente sua premiada segurança e gerenciamento de rede Quantum para redes públicas, privadas e híbridas na nuvem.

Segurança de rede em hiperescala

Maestro Orchestrator para o seu data center de última geração. A escalabilidade nunca foi tão fácil, dimensione os gateways de segurança Check Point existentes sob demanda.

Lightspeed Firewall

Os firewalls Quantum Lightspeed redefinem o desempenho do preço de segurança do data center com 250 a 800 Gbps de taxa de transferência de firewall com latência ultrabaixa de 3µ segundos.

Empresa high-end

26000/28000 Series

Quantum Security Gateways são as proteções mais abrangentes com hardware no nível de data center para maximizar o tempo de funcionamento e o desempenho.

Grandes Empresas

7000/16000 Series

Quantum Security Gateways proporcionam proteções de segurança abrangentes em uma configuração escalável e fácil de gerenciar, ideal para empresas grandes.

Médio e Enterprise

6000 Series

Quantum Security Gateways inclui a solução de segurança cibernética Gen V em um único gateway de segurança concebido para atender a todas as suas necessidades de negócios, hoje e no futuro.

Filial

Séries 1600/1800/3000

Quantum Security Gateways proporciona segurança no nível da empresa em uma plataforma compacta, ideal para filiais e escritórios pequenos.

Segurança para pequenas empresas

Séries 1500/1600/1800

Quantum Spark™ proporciona a segurança de nível empresarial mais abrangente para o seu negócio com gerenciamento e relatórios intuitivos e simples usando WebUI.

Dispositivos Industriais

1570R Modelos com e sem fio

Quantum Rugged proporciona uma prevenção de ameaças robusta de primeira linha para proteger os sistemas de controle industrial para manufatura, energia, serviços públicos e transporte.

Remote Access VPN

Quantum VPN fornece aos negócios de todos os tamanhos a habilidade de garantir conectividade e segurança, permitindo que a sua equipe se mantenha o mais produtiva possível.

IoT Security

De câmeras IP e elevadores inteligentes a dispositivos médicos e controladores industriais, a IoT Protect protege sua empresa contra ataques cibernéticos na rede e nos dispositivos.

Gateway virtual da filial

O Quantum Edge protege as filiais no local, com prevenção de ameaças de primeira linha que pode ser implantada dentro de minutos e gerenciada por uma plataforma unificada de prevenção e acesso a ameaças.

Segurança virtual: gateways e gerenciamento

Fornecendo a segurança mais inovadora e efetiva mantendo nossos clientes protegidos contra ataques virtuais de quinta geração.

Gerenciamento de segurança a partir da nuvem

Smart-1 Cloud é melhor gerenciamento de segurança disponível na nuvem

Dispositivos de gerenciamento de segurança

Os dispositivos Smart-1 são otimizados para gerenciamento de segurança em um único lugar, combinando gerenciamento de política, monitoramento e gerenciamento de eventos.

Gerenciamento de eventos

O SmartEvent, gerenciamento de ameaça é totalmente integrado, com registro, monitoramento, correlação de eventos e geração de relatórios em um único lugar.

4. SERVIÇOS ACTAR

Escopo do serviço de configuração inicial

Fase de discussões iniciais

- Reunião de Kick-off
- Apresentação do time
- Alinhamento de Escopo
- Definição de agenda de trabalho
- Reunião de Alinhamento Técnico
- Levantamentos das Informações Técnicas
- Entendimento da Topologia Final do Projeto
- Recebimento de pré-requisitos

Fase de planejamento

- Elaboração do HLD (Planejamento do Projeto)
- Elaboração do Cronograma
- Apresentação do Planejamento (HLD e Cronograma)

Fase de execução das configurações

- Configuração e migração dos equipamentos

Fase de finalização

- Documentação final do projeto.
- Reunião de Encerramento do Projeto

São entregáveis do serviço:

- Planejamento do Projeto (HLD)
- Cronograma de Atividades
- Documentação Final do Projeto

Premissas:

- A instalação física, a energização e o cabeamento de rede dos equipamentos é responsabilidade da CMBH;
- Está incluso nos valores apresentados nesta proposta, a alocação de um gerente de projetos para melhor desenvolvimento das atividades e cumprimentos dos prazos acordados;

- A CMBH deverá fornecer todas as informações e acessos físicos e lógicos ao profissional da ACTAR para o devido andamento do projeto;
- A CMBH deve disponibilizar técnico capacitado no local da instalação para apoio a equipe da ACTAR;
- É de responsabilidade da CMBH o devido funcionamento do(s) link(s) de internet da localidade de forma a possibilitar o acesso remoto e a agilidade nas atividades no tempo previsto de projeto.
- Na reunião de Kick-off serão definidas as atividades remotas e presenciais deste projeto.

Não-Escopo:

- Fornecimento de materiais de instalação, que não acompanhem os produtos adquiridos.
- Nenhuma outra configuração de quaisquer outras funcionalidades que não estejam citadas nos itens acima.
- Configurações em quaisquer outros dispositivos existentes na rede, que necessitem de intervenção, a fim de acomodar os firewalls, não estão inclusos no escopo desta proposta. (Ex. Switch, Roteador, etc.).

Escopo do serviço de Suporte técnico

A seguir demonstraremos as formas de atendimento, bem como a responsabilidade entre a ACTAR e a CMBH.

A descrição do serviço é subdividida nos seguintes itens:

- Tempo de Recuperação;
- Suporte Remoto 24x7;
- A cargo da ACTAR;
- A cargo da CMBH.

Suporte

As funções suportadas pelo Plano de Suporte serão executadas por uma estrutura organizacional específica para as diversas atividades de conteúdo técnico descritas neste escopo para os equipamentos fabricados pela Check Point localizados na rede da CMBH. A ACTAR disponibilizará 1 equipe (1 Base) de suporte, em regime de trabalho 24x7 (vinte e quatro horas por dia,

sete dias por semana) no caos de necessidade, para prover a suporte dos equipamentos da CMBH. A equipe será acionada a partir de um bilhete de defeito. Inicialmente o engenheiro de plantão da ACTAR tentará resolver a chamada remotamente (por telefone, e-mail ou sistema ACTAR).

No caso de não obter êxito durante o atendimento telefônico a ACTAR poderá enviar um engenheiro para atendimento on-site dentro dos prazos definidos no item de SLA.

O suporte técnico telefônico incluirá ajuda no uso de equipamento e software suportados. A referida assistência inclui auxílio na configuração, identificação de problemas no equipamento e/ou no software e trabalhos relacionados. A ajuda incluirá também diagnóstico de problemas ou download de atualizações de software.

São atividades de suporte técnico:

- Configurações locais para restabelecimento;
- Procedimentos de reinicialização dos equipamentos;
- Diagnóstico do sistema;
- Aplicação de correção de falhas de software;
- Procedimentos de liberação de alarmes;

Quando detectada a necessidade de troca de hardware, a CMBH fornecerá as peças necessárias, através do contrato entre a Check Point e a CMBH, para que o equipamento seja restabelecido. A troca deverá ser efetuada no próprio local pela CMBH, onde a ACTAR fará testes para verificar a funcionalidade do sistema.

Depois de realizado o atendimento, a equipe de suporte deverá informar à equipe de profissionais da CMBH os procedimentos operacionais realizados e eventuais problemas encontrados durante as atividades.

Tempo de Recuperação

Nos casos de alarme ou falha do sistema, a equipe de suporte atuará de acordo com os Tempos de Recuperação especificados a seguir, dependendo de cada ocorrência.

Entende-se por *"Tempo de Recuperação"* o intervalo de tempo, em horas ou fração, desde a abertura do bilhete de defeito pela CMBH até a normalização do sistema pela ACTAR, de forma que os usuários possam utilizá-lo com todos os recursos.

Para cada ocorrência é atribuída uma prioridade, classificada em quatro níveis, conforme descrito abaixo:

Falha Crítica

Ocorre em situações de alarme urgente em que há paralisação de equipamento(s), queda de um ou mais equipamentos no mesmo site ou em sites diferentes.

O sistema deverá ser restabelecido em até 4 (quatro) horas da abertura da chamada, sendo que teremos 2 (duas) horas para iniciarmos o atendimento e mais 2 (duas) para resolvermos o problema.

Falha Grave

Falha intermitente ou serviço degradado. Corresponde a situações de alarmes em que há riscos de degradação da qualidade. Este tipo de falha deverá ser solucionado em até 8 (oito) horas.

Falha Não Grave

Quando se perde a redundância (menor confiabilidade). São situações de alarme onde não ocorre paralisação ou degradação da qualidade do sistema, mas implica em redução da confiabilidade dos serviços. A confiabilidade deverá ser restabelecida em até 24 (vinte e quatro) horas.

Falha Leve

Não há risco iminente de degradação da qualidade ou confiabilidade do sistema, incluindo problemas de versões de software. Esta falha deverá ser solucionada em até 72 (setenta e duas) horas. Serão consideradas situações de exceção o atendimento de ocorrências que necessitem de pesquisa ou desenvolvimento de soluções, teste de meio de transmissão (elétrico ou óptico), os casos onde ocorram catástrofes, incêndios, inundações, infiltrações, terremotos, descargas atmosféricas, queda ou corte ou falha de energia elétrica e nos meios de transmissão dos locais onde se encontram instalados os equipamentos, falta de chave para acesso

ao local, não autorização de entrada ao local, chuva ou neblina em caso de serviços externos ou quando dificultarem o acesso ao local, trânsito intenso, barreiras em estradas, acidente com veículo da empresa ou de terceiros que possam impedir acesso da equipe ao local, falta de materiais para substituição, site localizado em local de risco, problemas de transmissão, problemas de infraestrutura ou outros que caracterizem um motivo de força maior para as quais os prazos definidos anteriormente não se aplicam.

A CARGO DA ACTAR

- Prestar serviços de suporte para a rede da CMBH por um período de 12 (doze) meses, a partir da assinatura do contrato entre CMBH e ACTAR.
- Informar à CMBH a pessoa que receberá os bilhetes de defeito (nomes, telefones fixos, celulares e e-mails), bem como a escala de acionamento para o caso de não ser possível contato com a primeira pessoa. Essa pessoa da ACTAR será responsável por acionar sua equipe de suporte em regime 24x7 (vinte e quatro horas por dia, durante sete dias por semana);
- Fornecer laptops, telefones celulares ou outros equipamentos para uso da equipe de suporte, durante a vigência do contrato;
- Responsabilizar-se pelos custos relativos a despesas decorrentes do trabalho a ser prestado;
- Fornecer mão de obra especializada;
- Divulgar, obrigatoriamente, instruções de segurança no início de trabalhos em campo;
- Executar os serviços de acordo com as especificações da CMBH e conforme os requisitos de qualidade e segurança recomendados pela Associação Brasileira de Normas Técnicas (ABNT) e/ou Órgãos Regulamentadores, atendendo à Legislação vigente;
- Responsabilizar-se em manter em estrita confidencialidade todas e quaisquer informações às quais tenha acesso em decorrência dos serviços a serem realizados e de todos os documentos, equipamentos e softwares colocados à disposição da CMBH, sendo expressamente vedada a sua reprodução ou divulgação para terceiros sem prévia autorização da CMBH, estando sujeita às sanções penais.

Considerações:

- Para atendimento on-site será contabilizado um mínimo de 4 (quatro) horas;
- Para atendimento remoto será contabilizado um mínimo de 2 (duas) horas;
- Os serviços considerados nesta proposta serão realizados na cidade de Belo Horizonte - MG;
- Esta proposta contempla a abertura de chamados junto o Technical Support Center do fabricante;
- Os valores deste contrato serão reajustados anualmente pela variação do IGPM em caso de continuidade do contrato por igual período.

Informações gerais:

- A ACTAR possui em seu quadro de funcional, somente profissionais contratados conforme CLT;
- Todos os profissionais possuem os seguintes benefícios: Bradesco Seguro Saúde, Bradesco Seguro Odontológico, Bradesco Vida e Vale-Refeição;
- A ACTAR ainda possui seguro de responsabilidade civil com abertura para imperícia na execução dos serviços prestados.

A CARGO DA CMBH

São de responsabilidade da CMBH:

- Fornecer a relação dos sites / prédios que serão atendidos por este escopo e autorização de entrada nos mesmos;
- Providenciar a troca dos equipamentos defeituosos junto ao fabricante;
- Designar no mínimo um contato básico e um contato reserva. A CMBH deve enviar um e-mail para a equipe de suporte técnico da ACTAR informando quaisquer modificações à lista inicial de contatos de abertura de chamada. Apenas os indivíduos designados nessa lista poderão contatar a equipe de suporte técnico da ACTAR;
- Fornecer os números de séries de todos os equipamentos e softwares de gerência cobertos no escopo dessa proposta;
- Manter ativo os contratos de suporte junto a Check Point.

Exclusões

A CMBH deverá disponibilizar todas as pessoas e/ou informações necessárias para a execução das tarefas envolvidas no suporte e suporte. Caso isto não seja possível em determinada situação, os impactos relativos a este atraso serão imputados à CMBH.

É de responsabilidade da CMBH a eventualidade de ocorrência de falhas ou danos às configurações geradas pelo uso indevido de sua equipe. Qualquer necessidade de novas instalações, serviços adicionais decorrentes de problemas causados pela CMBH, ou quaisquer outras atividades não incluídas nas ofertas de suporte desta proposta, poderão ser realizados após acordos comerciais realizados entre a ACTAR e CMBH.

5. TABELA DE VALORES

1) LICENCIAMENTOS CHECK POINT QUANTUM

12 MESES

PN	Descrição	Qtdade	Valor Un	Valor Total
CPAP-SG6400-PLUS-SNBT	6400 Plus appliance with SandBlast subscription package for 1 year	2	R$ 492.032,54	R$ 984.065,08
CPAP-NGSM600S-PLUS	Smart-1 600-S Plus Gen-6 Security Management,Log and SmartEvent appliance for 10 GWs (SmartEvent and Compliance 1 year)	1	R$ 136.742,68	R$ 136.742,68
CPCES-CO-PREMIUM-ADD	Collaborative Enterprise Support - Premium Add-on for Products	1	R$ 104.464,24	R$ 104.464,24
TOTAL				**R$ 1.225.272,00**

2) SERVIÇOS ACTAR

SET UP INICIAL	VALOR
Serviço de configuração das soluções CheckPoint; Implantação de licença de Mobile Access para criação de alta disponibilidade para o módulo de PVN existente; Configuração dos módulos de IPS, IA Application Control; Integração dos novos gateways a Gerência; Operação Assistida (serviço a ser realizado por profissionais certificados CheckPoint CCSE e CCSM)	R$ 55.442 ,00

SUPORTE TÉCNICO ACTAR	VALOR MENSAL	VALOR ANUAL
Serviço de Assistência Técnica e Suporte Técnico Remoto e On-Site (no local da CONTRATANTE) 24x7 (vinte e quatro horas por dia, sete dias por semana) com tempo de resposta para o primeiro atendimento em até quatro horas durante o período de vigência do contrato (serviço a ser realizado por profissionais certificados CheckPoint CCSE e CCSM)	R$ 7.240,00	R$ 86.880,00

6. CONDIÇÕES COMERCIAIS

1) Condições de Pagamento:

- **Equipamentos e licenças Check Point Quantum:** Os valores estão expressos em reais e serão faturados logo após a entrega das licenças e equipamentos.

- **Suporte Actar mensal**: O pagamento deverá ser efetuado mensalmente até o dia 05 de cada mês, com o pagamento a ser realizado em 30 (trinta) dias após o faturamento.

- **Acompanhamento de implantação** - O pagamento deverá ser efetuado ao final do serviço com pagamento realizado após 30 dias do faturamento, mediante depósito em conta corrente bancária da ACTAR ou outro meio acordado entre as partes, quando não for possível por depósito.

2) Impostos

Todos os impostos estão inclusos. Exceto diferencial de alíquota de ICMS. O Preço será alterado caso ocorram alterações nas alíquotas dos impostos.

3) Informações ACTAR

CNPJ para Faturamento do Software e serviços:

ACTAR Connectivity Engenharia de Telecomunicações Ltda
CNPJ: 00.085.885/0001-79
I.E: 062.889.097.007-2
Av.: Av do Contorno, 3772 - sala 1102 sala 1104– Santa Efigênia
Belo Horizonte - MG
CEP: 30110-022

Banco Itaú S/A
Ag 0587
C/C 34053-0

4) Validade da Proposta: 30 (trinta) dias.

5) Prazo de entrega: Em até 10(dez) dias úteis.

6) Aceite da Proposta: O pedido de compra ou a confirmação do fechamento do negócio deverá ser enviado para o e-mail aretuza.queiroz@actar.com.br.

At.te

Aretuza Queiroz
Diretoria Comercial
www.actar.com.br
aretuza.queiroz@actar.com.br
+55 31 99988-8747

RELATÓRIO DE ESTUDO TÉCNICO PRELIMINAR - ETP

Base legal: Lei Federal nº 14.133/2021

Segue o detalhamento dos cálculos dos valor apresentados na tabela do item **4 - ESTIMATIVA DO VALOR DA CONTRATAÇÃO** para as três propostas apresentadas:

Fornecedor 1 - Cyberone

Solução 1 - Valor Total: R$ 509.282,37

Detalhamento

R$404.882,37 - AS-IS-VENDA (pg.14 da proposta comercial)
R$18.000,00 - Serviço de Instalação (pg.16 da proposta comercial)
R$86.400,00 - Serviço de Suporte (pg.16 da proposta comercial)

Solução 2 - **Valor Total: R$ 603.034,80**

Detalhamento

pg.14 da proposta comercial

Fornecedor 2 - Altasnet

Solução 1 - Valor Total: R$795.900,00

Detalhamento

pg.10 da proposta comercial “FORNECIMENTO DE CLUSTER DE FIREWALL

R$515.680,00 - Item 1 da proposta comercial
R$685.140,00/3 - Item 1.1 da proposta comercial proporcional a 12 meses
R$ 26.880,00 - Item 3 da proposta comercial
R$74.880,00/3 - Item 3 da proposta comercial proporcional a 12 meses

O item 2 foi desconsiderado por não fazer parte do escopo do estudo técnico preliminar.

Solução 2 - Valor Total: R$581.172,00

Detalhamento

pg.10 da proposta comercial “LOCAÇÃO DE CLUSTER DE FIREWALL”

O valor apresentado na proposta comercial é unitário mensal, para 36 meses. Todos os itens foram considerados no cálculo, exceto o item 2 que não faz parte do escopo do estudo técnico preliminar.

Valor mensal: R$48.431,00 = R$50.356,00 - 1.925,00 (item 2)

Valor 12 meses: R$581.172,00 = R$48.431,00 x 12

Fornecedor 3 - Actar

Solução 1 - Valor Total: R$1.367.594,00

Detalhamento

Foram somados os itens 1 e 2 presentes no tópico 5 da proposta comercial

R$1.367.594,00 =1.225.272,00 + 55.442,00 + 86.880,00