TIPO: CPS
Nº: 110/2024

CONTRATO que entre si celebram o Serviço Nacional de Aprendizagem do Cooperativismo de Minas Gerais – SESCOOP/MG e PROCEDATA INFORMÁTICA LTDA.

CLAUSULA PRIMEIRA: DAS PARTES

1.1. **SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO DE MINAS GERAIS – SESCOOP/MG**, doravante denominado **CONTRATANTE**, situado na Rua Ceará, nº 771, Bairro Santa Efigênia, Cidade Belo Horizonte/MG – CEP 30.150-312, inscrita no CNPJ nº 07.064.534/0001-20 e Inscrição Estadual Isento, neste ato representado pelo seu superintendente ALEXANDRE GATTI LAGES, portador do CPF nº 005.XXX.3XX-22 e por sua gerente geral ISABELA CHENNA PEREZ, portadora do CPF nº 074.XXX.7XX-85.

1.2. **PROCEDATA INFORMÁTICA LTDA,** doravante denominada **CONTRATADA,** situada na Av. Nossa Senhora do Carmo, nº 45, salas 501 a 504, Bairro Carmo Sion, CEP 30.310-000, Belo Horizonte/MG, inscrita no CNPJ 65.181.075/0001-61, representada neste ato por FERES MARON SALIM, portador do CPF nº 716.XXX.1XX-87.

CLÁUSULA SEGUNDA: DO OBJETO

2.1. Constitui objeto deste **CONTRATO** a prestação de serviços fornecimento de software, hardware, serviço de instalação, migração, configuração e otimização para solução de firewall, modelo SonicWall Gen 7 NSa 2700, com alta disponibilidade (HA – High Availability), contendo Advanced Protection Security Suite, pelo período de 36 (trinta e seis) meses, incluindo o suporte técnico do fabricante por igual período, para atender as necessidades do **CONTRATANTE**.

CLÁUSULA TERCEIRA: ESCOPO DA EXECUÇÃO DOS SERVIÇOS

3.1. Os equipamentos e softwares deverão ser entregues no prazo máximo de 45 (quarenta e cinco) dias úteis, e os serviços realizados, inclusive documentação, no prazo máximo de 30 (trinta) dias úteis após entrega dos equipamentos / softwares, diretamente na Sede do **CONTRATANTE**, localizada na Rua Ceará, nº 771, Bairro Santa Efigênia, CEP 30150-311, em Belo Horizonte/MG.

> 3.1.1. O prazo se inicia a partir da data de vigência prevista na cláusula sétima, deste contrato.

3.2. Previamente à entrega/execução dos serviços, a **CONTRATADA** deverá obrigatoriamente, efetuar contato com a Gerência de Tecnologia da Informação (GETIN) do **CONTRATANTE**, cujos dados para contato são: getin@sistemaocemg.coop.br e moacir.junior@sistemaocemg.coop.br, visando pactuar as especificidades da entrega/execução dos serviços e demais informações que se fizerem necessárias.
3.3. Por ocasião da entrega dos equipamentos/softwares e realização dos serviços, a **CONTRATADA** deverá observar rigorosamente as especificações técnicas descritas na cláusula décima. A não obediência a este quesito acarretará a devolução sumária dos equipamentos/serviços e a aplicação das penalidades cabíveis.
3.4. Os equipamentos entregues deverão ser novos, de 1º uso e em linha de produção mais recente, igual ou superior tecnologicamente, à época de aquisição, não sendo aceito equipamentos utilizados em exposições, feiras ou eventos promocionais.
3.5. Os equipamentos entregues em desconformidade com as especificações especificadas neste contrato serão passíveis de devolução à **CONTRATADA**, cabendo a esta todo e quaisquer ônus decorrentes, inclusive, se for o caso, o cancelamento de Nota Fiscal, mesmo que emitida em mês anterior, ficando entendido que a entrega de equipamentos em desconformidade é considerada falta grave, podendo ensejar a aplicação das penalidades cabíveis.

3.6. Os equipamentos entregues estão sujeitos à inspeção pelo **CONTRATANTE**, que poderá rejeitá-los (no todo ou em parte) se considerá-los defeituosos ou divergentes com relação às especificações. Os equipamentos rejeitados serão restituídos à **CONTRATADA**, por sua conta e risco. Todas as despesas com desembalagem, reembalagem e devolução dos equipamentos serão debitadas à **CONTRATADA**.
3.7. A realização dos serviços deverá ser efetuada por técnicos da **CONTRATADA**/fabricante, sendo acompanhada por técnicos indicados pelo **CONTRATANTE**.
3.8. O atraso na entrega dos equipamentos/softwares e execução dos serviços ensejará a aplicação da multa, conforme previsto neste contrato.
3.9. Eventuais solicitações de prorrogação do prazo de entrega somente serão analisadas se atenderem às seguintes condições:

a) O pedido for encaminhado à Comissão Permanente de Licitação, sendo desconsiderados para efeito de isenção de multa, os pedidos encaminhados diretamente à outras Gerências do **CONTRATANTE**, mesmo que deferidos;
b) O pedido for enviado à Comissão Permanente de Licitação antes de expirada a data de entrega **CONTRATADA**. Vencida a data de entrega não haverá isenção de multas;
c) O eventual atraso decorrer de caso fortuito ou força maior, assim entendidas as circunstâncias absolutamente imprevisíveis e insuperáveis por parte da **CONTRATADA**. A falta de programação, ou acordo, ou entendimento entre a **CONTRATADA** e seus fornecedores/fabricantes não são motivos para prorrogação da data.

3.10. O pedido de prorrogação será analisado pela Comissão Permanente de Licitação, podendo ser deferido ou indeferido, formalmente, ficando certo e esclarecido que o indeferimento não desobriga a **CONTRATADA** de entregar os equipamentos, sujeitando-se a mesma, neste caso, às penalidades cabíveis. A negativa de entrega, em face do indeferimento, será considerada falta grave, podendo ensejar a suspensão do direito de licitar e contratar com o SESCOOP, nos termos de seu regulamento.
3.11. A aceitação dos equipamentos/serviços não exime a **CONTRATADA** da responsabilidade quanto à qualidade dos mesmos e não invalida qualquer reclamação posterior do **CONTRATANTE**.
3.12. A **CONTRATADA** deverá executar todo o serviço necessário a plena operacionalização da solução ofertada, devendo obrigatoriamente incluir todos os serviços abaixo:

a) Reunião de Quick off do projeto;
b) Planejamento detalhado dos procedimentos a serem executados;
c) Apresentação ao cliente do cronograma e processos para aprovação;
d) Instalação física dos componentes de hardware fornecidos no rack do **CONTRATANTE**;
e) Interligação dos componentes de hardware fornecidos a rede/links do **CONTRATANTE** de forma redundante;
f) Prestar auxílio em qualquer configuração de rede necessária a instalação da solução;
g) Instalação do licenciamento necessário;
h) Atualização de firmware dos componentes de hardware fornecidos;
i) Configuração da alta disponibilidade do hardware fornecido;
j) Levantamento de todas as regras de firewall, filtros de conteúdo, IPS, IDS, anti-malware e demais proteções existentes nos firewalls antigos do **CONTRATANTE**;
k) Migração, ajustes e otimização de todas as regras de firewall e demais configurações de controle e segurança aos novos firewalls;
l) Criar ou ajustar novas políticas de segurança conforme definição do **CONTRATANTE**;
m) Criar ou ajustar novas regras de firewall conforme definição do **CONTRATANTE**;
n) Implementar, criar ou ajustar um ambiente seguro de Captive Portal corporativo seguindo as melhores práticas;
o) Configurar e atualizar os relatórios existentes no software Global Management System (GMS) atualmente instalado e licenciado no **CONTRATANTE**;

p) Proceder a testes de funcionalidade antes da entrada em produção;
q) Proceder o acompanhamento da entrada em produção de forma presencial ou remota, dependendo da criticidade no ambiente do **CONTRATANTE**, com no mínimo 7 dias de acompanhamento;
r) Proceder aos ajustes necessários para solução dos problemas apresentados durante a entrada em produção;
s) Proceder a documentação completa contendo o passo a passo da nova solução instalada;
t) Proceder a um treinamento hands-on de no mínimo 8 horas sobre a solução instalada, incluindo o gerenciamento básico dos recursos migrados/ativos da solução de firewall, relatórios;
u) A **CONTRATADA** deverá obrigatoriamente registar os novos equipamentos na conta institucional do **CONTRATANTE** no site MySonicWall (https://www.mysonicwall.com/).

3.13. Quaisquer outros serviços necessários ao pleno funcionamento da solução deverão ser executados pela **CONTRATADA** mesmo que não estejam listados acima.
3.14. Todos os serviços devem ser executados de forma a não gerar paradas no ambiente de produção do **CONTRATANTE** durante o horário comercial. Serviços com risco ou necessidade de parada do ambiente de produção, deverão obrigatoriamente ser executados fora de horário comercial.
3.15. A **CONTRATADA** deve estar ciente que o **CONTRATANTE** não executará serviços que só podem ser realizados presencialmente. De forma explicita ficam definidos que os serviços de instalação física, serão obrigatoriamente executados de forma presencial no endereço do **CONTRATANTE** e não permitem negociação de atendimento remoto pela **CONTRATADA**.
3.16. A **CONTRATADA** deverá fornecer 04 (quatro) cabos de conexão direta DAC SFP 10G 1,0 metro.

CLÁUSULA QUARTA: DO PREÇO E FORMA DE PAGAMENTO

4.1. Para a realização do objeto deste **CONTRATO**, o **CONTRATANTE** repassará à **CONTRATADA**, o valor estimado total de **R$ 106.900,00 (cento e seis mil, novecentos reais),** conforme valores unitários especificados abaixo:

Item	Qtde.	Descrição	Valor Unitário	Valor Total
1	1	SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante) com garantia de 3 anos do fabricante.	-	R$ 19.287,86 (dezenove mil duzentos e oitenta e sete reais e oitenta e seis centavos).
2	1	SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability) com garantia de 3 anos do fabricante.	-	R$ 21.944,17 (vinte e um mil novecentos e quarenta e quatro reais e dezessete centavos).
3	1	Software Advanced Protection Security Suite com suporte técnico de 3 anos do fabricante.	-	R$ 42.387,74 (quarenta e dois mil trezentos e oitenta e sete reais e setenta e quatro centavos).
4	1	Serviço de instalação/migração, configuração e otimização.	-	R$ 21.639,15 (vinte e um mil seiscentos e trinta e nove reais e quinze centavos).
5	4	Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	R$ 410,27 (quatrocentos e dez reais e vinte e sete centavos).	R$ 1.641,08 (um mil seiscentos e quarenta e um reais e oito centavos).

4.2. O faturamento ocorrerá 100% (cem por cento) após a realização da entrega dos equipamentos/softwares, bem como realização dos serviços. Sendo o pagamento efetuado no

prazo máximo de 28 (vinte oito) dias corridos, mediante a apresentação da Nota Fiscal/Fatura pela **CONTRATADA**, devidamente aprovada pela Gerência de Licitações e Compras do **CONTRATANTE**, sem prejuízo de eventuais multas por atraso.
4.3. A nota fiscal / fatura deverá ser encaminhada para o e-mail notasfiscais@sistemaocemg.coop.br contendo os dados bancários para pagamento, que será realizado preferencialmente via depósito em conta.
4.4. No caso de emissão de Nota Fiscal na forma "eletrônica", a **CONTRATADA** fica obrigada a enviar juntamente com o documento o arquivo eletrônico denominado "XML" para fins de conferência e fechamento junto a receita estadual. A Nota Fiscal ficará retida para pagamento, até o envio do presente arquivo.
4.5. Não será aceita Nota Fiscal / Fatura de serviços emitida entre o dia 21 e 31 de determinado mês. A ocorrência de tal fato implicará na devolução sumária, ficando a **CONTRATADA** obrigada a substituir o documento.
4.6. O **CONTRATANTE** poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela empresa **CONTRATADA**, nos termos deste contrato.
4.7. No caso de incorreção na Nota Fiscal, esta será restituída à **CONTRATADA** para as correções solicitadas. O prazo de pagamento será contado a partir da data da regularização do documento fiscal, não respondendo o **CONTRATANTE** por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.
4.8. Caso os equipamentos e serviços constantes da Nota Fiscal/Fatura estejam em desacordo com os equipamentos entregues/serviços executados, ela não será liberada para pagamento, até a correção do fato. Caberá à **CONTRATADA** a solução do problema para aprovação dos equipamentos/serviços pelo **CONTRATANTE** e liberação do pagamento.
4.9. O **CONTRATANTE** fará a retenção dos impostos de acordo com a legislação vigente, caso aplicável.

4.9.1. Retenção de Imposto Sobre Serviço de Qualquer Natureza (ISSQN): de acordo com a Legislação, as Microempresas ou as Empresas de Pequeno Porte, optantes pelo Simples Nacional, que não informarem, a alíquota de retenção nos documentos fiscais, será aplicada a alíquota de 5% (cinco por cento).

4.10. A Nota Fiscal/Fatura deverá ser emitida pela **CONTRATADA**, obrigatoriamente com o número de inscrição do CNPJ apresentado no processo de contratação, não se admitindo Nota Fiscal/Fatura emitida com outro CNPJ, mesmo de filiais ou da matriz da **CONTRATADA**.
4.11. Salvo autorização expressa e por escrito do **CONTRATANTE**, é vedado à **CONTRATADA**, seja por qual motivo for, o desconto ou negociação de duplicatas, faturas e afins em instituições financeiras, relativamente a parcelas de pagamento vinculadas ao fornecimento / execução dos serviços do objeto deste contrato.

CLÁUSULA QUINTA: DA RESCISÃO

5.1. Qualquer dos partícipes poderá denunciar o presente CONTRATO por meio de comunicação escrita, com antecedência mínima de 10 (dez) dias. Ficando as partes responsáveis pelas obrigações decorrentes do tempo de vigência e creditando-lhes, igualmente, os benefícios adquiridos no mesmo período.
5.2. Constitui motivo para rescisão deste CONTRATO, independentemente do instrumento de sua formalização, o inadimplemento de qualquer item pactuado, particularmente quando constatadas as seguintes situações:

5.2.1. Não cumprimento de cláusulas ou prazos constantes neste CONTRATO;
5.2.2. Cumprimento irregular das cláusulas ou prazos constantes deste CONTRATO;
5.2.3. Paralisação da execução do objeto deste CONTRATO, sem a justa causa e prévia comunicação ao **CONTRATANTE**;
5.2.4. A associação da **CONTRATADA** com outrem, ainda a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não são admitidas neste CONTRATO;

5.2.5. Desatendimento das determinações regulares da autoridade designada para acompanhar a execução deste CONTRATO, assim como a de seus superiores;
5.2.6. Cometimento reiterado das faltas na execução deste CONTRATO;
5.2.7. Alteração social ou modificação da finalidade ou da estrutura da instituição que, a juízo do **CONTRATANTE**, prejudique a execução do objeto deste CONTRATO;
5.2.8. A ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditiva da execução deste CONTRATO;
5.2.9. Prática de atos ilícitos visando frustrar os objetivos deste CONTRATO;
5.2.10. Cometimento de falhas ou fraudes na execução do objeto deste CONTRATO;
5.2.11. Inadimplência total do objeto deste CONTRATO.

5.3. Os casos de rescisão serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa, no prazo de 10 (dez) dias, a contar do recebimento da notificação extrajudicial.
5.4. Se o presente CONTRATO for rescindido, o Termo de Rescisão deverá discriminar:

5.4.1. Balanço dos eventos já cumpridos ou parcialmente cumpridos; e
5.4.2. Relação dos pagamentos já efetuados ou ainda devidos.

CLÁUSULA SÉXTA: DO ACOMPANHAMENTO

6.1. Ao **CONTRATANTE** fica assegurado o direito de exercer controle e fiscalização sobre a execução dos trabalhos desenvolvidos pela **CONTRATADA**, através da Gerência da Tecnologia da Informação (GETIN), através do empregado MOACIR LOURENÇO ROSA JUNIOR, ou na falta deste, por quem o **CONTRATANTE** indicar para cumprir a função, assim como questionar quaisquer eventualidades que desvirtuem o caráter intrínseco do mesmo.
6.2. Caberá à **CONTRATADA** apresentar responsável pelo acompanhamento do projeto apresentado.
6.3. Caso a **CONTRATADA**, no decorrer da prestação dos serviços, demonstre inaptidão técnica, operacional ou administrativa, bem como quaisquer outras características que, no entendimento do **CONTRATANTE**, possa prejudicar, inviabilizar, retardar ou desvirtuar o objetivo pretendido, poderá a entidade aplicar as penalidades previstas no presente Contrato.
6.4. A gestão corporativa do contrato será realizada pela Gerência de Licitações e Compras (GELIC).

CLÁUSULA SÉTIMA: DA VIGÊNCIA

7.1. O prazo de vigência deste **CONTRATO** será de 07 (sete) meses, iniciar-se-á na data de 29 de julho de 2024 e findar-se-á em 28 de fevereiro de 2025, podendo ser prorrogado, mediante acordo prévio entre as **PARTES**, retratado através de Termo Aditivo.

CLÁUSULA OITAVA: DOS ENCARGOS

8.1. Será de exclusiva responsabilidade da **CONTRATADA** o pagamento dos encargos trabalhistas, previdenciários e aqueles relacionados à prevenção de acidentes de trabalho, de seus funcionários, não decorrendo do presente CONTRATO, qualquer vínculo empregatício com o **CONTRATANTE** ou eventuais prepostos.

8.1.1. Fica expressamente convencionado que, na hipótese de uma das partes ser autuada, notificada, intimada ou condenada, por qualquer obrigação comprovadamente de responsabilidade da outra parte, seja de que natureza for, mesmo após o término do CONTRATO, a parte inocente deverá notificar a parte infratora para que esta, no prazo de até 30 (trinta) dias, contados do recebimento de tal notificação, cumpra a obrigação determinada;

8.1.2. Caberá à **CONTRATADA**, informar aos seus parceiros e empregados envolvidos na execução das ações educativas, o conteúdo do presente CONTRATO.

8.2. A **CONTRATADA** deverá efetuar, por sua conta, o pagamento dos impostos, licenças e taxas federais, estaduais e municipais, incidentes sobre sua atividade ou decorrentes desta parceria, comprovando tais pagamentos ao **CONTRATANTE** ou, reconhecimento de isenções e imunidades, sempre que este solicitar, formalmente.

CLÁUSULA NONA: PENALIDADES

9.1. A inexecução total ou parcial injustificada, a execução deficiente, irregular ou inadequada do objeto do presente contrato, assim como o descumprimento dos prazos e condições estipulados e, sem prejuízo, implicarão nas penalidades abaixo mencionadas:

9.1.1. Advertência;
9.1.2. Cancelamento do contrato;
9.1.3. Multa por não realização dos serviços;
9.1.4. Suspensão do direito de licitar ou contratar com o Sescoop, por prazo não superior a 5 (cinco) anos.
9.1.5. Será cobrada multa por atraso na entrega dos equipamentos e softwares e na execução dos serviços, no percentual de 0,5% (meio por cento) ao dia, referente a parcela em atraso, limitada a 10% (dez por cento) do valor total do CONTRATO.

9.2. Ocorrendo a aplicação de multa, esta será descontada sobre o valor da nota fiscal/fatura ou dos créditos a que a empresa **CONTRATADA** fizer “jus”, no ato do pagamento, ou recolhidas diretamente à tesouraria do **CONTRATANTE**, ou ainda, quando for o caso, cobrada judicialmente;
9.3. Para aplicação das penalidades aqui previstas, a **CONTRATADA** será notificada para apresentação de defesa prévia, no prazo de 05 (cinco) dias, contados da notificação.
9.4. As penalidades previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis, tal como a rescisão contratual.

CLÁUSULA DÉCIMA: ESPECIFICAÇÃO TÉCNICA DA FERRAMENTA FIREWALL

10.1. Compete a **CONTRATADA** fornecer os seguintes itens para execução do objeto:

PRODUTO SOLUÇÃO DE FIREWALL	QUANTIDADE
SonicWall Gen 7 NSa 2700 appliances 01 (ou superior do mesmo fabricante).	01
SonicWall Gen 7 NSa 2700 appliances 02 (HA – High Availability).	
Software Advanced Protection Security Suite.	
Garantia do fornecedor (3 anos).	
Suporte técnico do fornecedor (3 anos).	
Serviço de instalação/migração, configuração e otimização.	
Fornecimento de 04 Cabos de Conexão Direta DAC SFP 10G 1,0 Metro.	04

10.2. Os equipamentos e serviços deverão preencher os seguintes requisitos mínimos:

10.2.1. O equipamento deve ser obrigatoriamente novo, em linha de montagem e de primeiro uso, podendo, a critério da empresa **CONTRATADA**, utilizar ou não o sistema de benefícios SonicWall Secure Upgrade appliance.
10.2.2. Fornecimento e instalação do software de segurança Advanced Protection Security Suite com todas suas features habilitadas durante 3 (três) anos em ambos os appliances fornecidos na solução com alta disponibilidade (HA).

10.2.3. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.
10.2.4. Desempenho em modo de Inspeção (descriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.
10.2.5. Desempenho mínimo de 3.4 Gbps de IPS.
10.2.6. Suporte mínimo de 1.500.000 conexões simultâneas/concorrentes no modo SPI.
10.2.7. Suporte mínimo de 21.000 novas conexões por segundo.
10.2.8. Deve possuir armazenamento interno de no mínimo 64 GB e suportar expansão de armazenamento interno para até 256Gb.
10.2.9. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.
10.2.10. Deve possuir 16 interfaces 1 GbE padrão RJ-45.
10.2.11. Deve possuir 3 interfaces 10GbE SFP+.
10.2.12. Deve possuir 1interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.
10.2.13. Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.
10.2.14. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos.
10.2.15. A VPN SSL deve ser licenciada para, no mínimo, 02 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos.
10.2.16. Deve suportar 2000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.
10.2.17. Deve suportar, no mínimo, 2.1Gbps de desempenho de VPN IPSEC.
10.2.18.O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.
10.2.19. O Equipamento deverá ser homologado pela ANATEL.
10.2.20. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.
10.2.21. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 36 (trinta e seis) meses.
10.2.22. É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

10.3. Os FIREWALLS FÌSICOS deverão preencher as seguintes características e especificações:

10.3.1. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.
10.3.2. Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.
10.3.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
10.3.4. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

10.3.5. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.
10.3.6. Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 36 meses, incluindo garantia e suporte.
10.3.7. Deverá ser fornecido suporte técnico com a fabricante do produto durante 36 meses no mínimo.

10.4. A **CONTRATADA** deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.
10.5. A **CONTRATADA** deve implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.
10.6. A **CONTRATADA** deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
10.7. A **CONTRATADA** deve fornecer proteção anti-spoofing.

10.8. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;
10.9. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.
10.10. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.
10.11. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.
10.12. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

a) Latência;
b) Jitter;
c) Perda de pacotes.

10.13. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico.
10.14. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.
10.15. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.
10.16. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
10.17. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
10.18. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.
10.19. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.
10.20. Deve suportar DHCP relay.
10.21. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz

de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.
10.22. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.
10.23. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.
10.24. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.
10.25. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

10.26. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood etc.
10.27. Detectar e bloquear a origem de portscans.
10.28. Deve permitir o bloqueio de ataques.
10.29. Deve permitir o bloqueio de exploits conhecidos.
10.30. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP.
10.31. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser descriptografado de forma transparente à aplicação.
10.32. Implementar DSCP (Differentiated Services Code Points).
10.33. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.
10.34. Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.
10.35. Implementar mecanismo de sincronismo de horário através do protocolo NTP.
10.36. Possuir suporte ao protocolo SNMP versões 2 e 3.
10.37. Possuir suporte a log via syslog.
10.38. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.
10.39. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período, e baseado em normas nacionais e internacionais de segurança da informação.
10.39. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.
10.40. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

10.41. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.
10.42. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.
10.43. Deve permitir a funcionalidade de ARP bridging.
10.44. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".
10.45. A **CONTRATADA** deverá fornecer o VPN com as seguintes características:

10.45.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
10.45.2. Suportar algoritmos de criptografia 3DES, AES 128 e AES 256.
10.45.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.
10.45.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.
10.45.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.
10.45.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.
10.45.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.
10.45.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.
10.45.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
10.45.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.
10.45.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.
10.45.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.
10.45.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.
10.45.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.
10.45.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.
10.45.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

10.46. DA ALTA DISPONIBILIDADE (HA)

10.46.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.
10.46.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.

10.46.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.
10.46.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.
10.46.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.
10.46.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.
10.46.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.
10.46.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.
10.46.9. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

10.47. DO CONTROLE DE AMEAÇAS

10.47.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.
10.47.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.
10.47.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.
10.47.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”.
10.47.5. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.
10.47.6. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.
10.47.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.
10.47.8. Implementar interface CLI segura através do protocolo SSH.
10.47.9. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.
10.47.10. A solução deve permitir criar regras de exceção de acordo com a proteção.
10.47.11. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;
10.47.12. Permitir o bloqueio de malwares (vírus, worms, spyware etc.).
10.47.13. A solução deve ser capaz de proteger contra-ataques a DNS.
10.47.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.
10.47.15. A solução deve ser capaz de prevenir acesso a websites maliciosos.
10.47.16. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.
10.47.17. A solução deverá receber atualizações de um serviço baseado em cloud.
10.47.18. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

10.47.19. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.
10.47.20. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.
10.47.21. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.
10.47.22. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

10.48. PROTEÇÃO CONTRAATAQUES AVANÇADOS

10.48.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.
10.48.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.
10.48.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.
10.48.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.
10.48.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.
10.48.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.
10.48.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.
10.48.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.
10.48.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.
10.48.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.
10.48.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.
10.48.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego.
10.48.13. Conter ameaças avançadas de dia zero.
10.48.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.
10.48.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos.
10.48.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.
10.48.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

10.48.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.
10.48.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS.
10.48.20. Mitigar ameaças de dia zero de forma transparente para o usuário final.
10.48.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.
10.48.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.
10.48.23. Mitigar ameaças de dia zero via tráfego de internet.
10.48.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.
10.48.25. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.
10.48.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.
10.48.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.
10.48.28. Conter e mitigar exploits avançados.
10.48.29. A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).
10.48.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.
10.48.31. As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.
10.48.32. A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering.
10.48.33 .A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.
10.48.34. A Solução deve unificar diversas funções de segurança em um único conjunto integrado inspecionando os arquivos de usuários locais, remotos e móveis.
10.48.35. A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS etc., sem afetar o desempenho.
10.48.36. A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças , com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

a) Inspeção profunda de memória em tempo real;
b) Inspeção profunda de pacotes livre de remontagem;
c) Descriptografia e inspeção TLS/SSL;
d) Inteligência e controle de aplicativos;
e) Recursos SD-WAN seguros.

10.48.37. É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

10.49. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

10.49.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.
10.49.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local.
10.49.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.
10.49.4. Permitir a customização de página de bloqueio.
10.49.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.
10.49.6. Deve permitir submissão de novos sites para categorização.
10.49.7. Permitir a classificação dinâmica de sitesweb, URLs e domínios.
10.49.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.
10.49.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.
10.49.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

10.50. CARACTERÍSTICAS DE AUTENTICAÇÃO

10.50.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.
10.50.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.
10.50.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.
10.50.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.
10.50.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.
10.50.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW.
10.50.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.
10.50.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.
10.50.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.
10.50.10. A solução deve possibilitar SSO via API.

10.51. CARACTERÍSTICAS DE ADMINISTRAÇÃO

10.51.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.
10.51.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.
10.51.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.
10.51.4. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração.
10.51.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.
10.51.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.
10.51.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.
10.51.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.
10.51.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.
10.51.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.
10.51.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.
10.51.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.
10.51.13 Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.
10.51.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilzida por política, por protocolo TCP/UDP IPV4 e IPV6.
10.51.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.
10.51.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).
10.51.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.
10.51.18. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.
10.51.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

10.51.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.
10.51.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.
10.51.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.
10.51.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.
10.51.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.
10.51.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.
10.51.26. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto provisionamento da plataforma através de ponto central de gerenciamento.
10.51.27. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações
10.51.28. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.
10.51.29. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

CLÁUSULA DÉCIMA PRIMEIRA: DA CONFIDENCIALIDADE

11.1. As PARTES reconhecem que todas as informações, de qualquer natureza, eventualmente reveladas pelas partes, sejam feitas em meio físico, magnético ou oralmente, durante a vigência do presente contrato, incluídas, mas não se limitando à base de dados técnicos, planos comerciais ou estratégicos, informações financeiras e projeções, dados ou informações sobre o mercado, clientes, parceiros, fornecedores ou equipamentos, documentos, projetos, ou até mesmo correspondências classificadas como informações confidenciais e sobre as mesmas deverá ser guardado sigilo absoluto, para todos os efeitos.
11.2. A obrigação de confidencialidade de que trata o presente contrato visa proteger os direitos e interesses de todo gênero das partes, buscando impedir a revelação e a utilização indevida das Informações Confidenciais, motivo pelo qual as partes obrigam-se, de forma perene, em caráter irretratável e irrevogável, a manter sob sigilo absoluto todas as Informações Confidenciais a que vier a ter acesso, tratando-as como segredo industrial e de negócios.
11.3. É vedado à **CONTRATADA** divulgar informação, dado ou modelo que tenha sido desenvolvido a partir de qualquer Informação Confidencial, bem como desenvolver produtos, métodos ou serviços com base tanto nas Informações Confidenciais, como nas demais informações e conhecimentos obtidos no desenvolvimento do propósito deste contrato, sem qualquer exceção.
11.4. A **CONTRATADA** declara-se ciente e concorda, bem como adotará todas as medidas para deixar seus parceiros, Colaboradores e clientes também cientes, e que a executora em decorrência do presente contrato poderá ter acesso, utilizará, e processará, eletrônica e manualmente, informações e dados prestados pela executora e seus clientes (“Dados Protegidos”).
11.5. As Partes declaram-se cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) (“LGPD”), e obrigam-se a adotar todas as medidas razoáveis par garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD.
11.6. As Partes declaram-se cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) (“LGPD”), e se comprometem a

realizar o tratamento de Dados Pessoais aos quais obtenham acesso em decorrência deste Contrato de acordo com a legislação aplicável, incluindo, mas não se limitando à Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), Lei 12.965/2014 (Marco Civil da Internet), Decreto n. 8.771/2016 (Regulamento do Marco Civil da Internet), bem como quaisquer outras leis ou normas relativas à proteção de dados pessoais que vierem a ser promulgadas ou entrarem em vigor no curso da vigência deste contrato. E obrigam-se a adotar todas as medidas razoáveis par garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD.

11.7. O **CONTRATANTE** está comprometido em assegurar que o controle sobre os dados pessoais. Para isso, atua fortemente para garantir que sua privacidade e a proteção dos seus dados pessoais sejam observadas quando você está nos nossos ambientes físicos ou quando acessa nossos ambientes digitais. Coletamos e tratamos os dados pessoais, de acordo com nosso Aviso de Privacidade disponível em: https://sistemaocemg.coop.br/evento/portal-da-privacidade/?categories=10%3B e em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD, o Marco Civil da Internet e outras Leis ou regulamentos aplicados ao tema.

11.8. A **CONTRATADA** declara estar ciente que quaisquer comunicações e/ou solicitações relacionadas à proteção de dados pessoais decorrentes do presente instrumento deverão ser realizadas exclusivamente através do canal oficial estabelecido pelo SESCOOP/MG: dpo@sistemaocemg.coop.br.

11.9. A **CONTRATADA** declara-se ciente e concorda, bem como adotará todas as medidas para deixar seus parceiros, Colaboradores e clientes também cientes, e que a **CONTRATADA** em decorrência do presente contrato poderá ter acesso, utilizará, e processará, eletrônica e manualmente, informações e dados prestados pela executora e seus clientes (“Dados Protegidos”).

11.10. As PARTES declaram-se cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais – “LGPD” (Lei 13.709/2018), e obrigam-se a adotar todas as medidas razoáveis par garantir, por si, bem como seu pessoal, colaboradores, empregados e subcontratados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD, nos termos do ANEXO I e II.

CLÁUSULA DÉCIMA SEGUNDA: DAS OBRIGAÇÕES DAS PARTES

12.1. **DO CONTRATANTE:**

12.1.1. Acompanhar a execução de todo o trabalho desenvolvido, assim como questionar quaisquer eventualidades que desvirtuem o seu caráter intrínseco;

12.1.2. Prestar as informações e os esclarecimentos que forem solicitados pela **CONTRATADA** durante o prazo de vigência do Contrato;

12.1.3. Proporcionar todas as facilidades para que a **CONTRATADA** possa desempenhar seus serviços dentro do especificado neste **CONTRATO**;

12.1.4. Efetuar os pagamentos conforme clausula 4ª do presente contrato;

12.2. **DA CONTRATADA**:

12.2.1. Executar o objeto do presente **CONTRATO** desenvolvendo conteúdos próprios para realização dos módulos e aplicação do conteúdo mediante prévia aprovação do **CONTRATANTE**;

12.2.2. Prestar serviços dentro dos parâmetros e rotinas estabelecidos, com observância às recomendações aceitas pela boa técnica de procedimentos, das normas que regulamentam o objeto;

12.2.3. Manter absoluto sigilo sobre quaisquer informações de que venha a tomar conhecimento ou ter acesso quando da execução do objeto do presente instrumento;

12.2.4. Arcar com a responsabilidade civil por todos e quaisquer danos materiais e morais causados pela ação ou omissão de seus empregados, trabalhadores, prepostos ou representantes, dolosa ou culposamente, à **CONTRATANTE**.

12.2.5. Cumprir fielmente com o CONTRATO, prestando os serviços com respeito às Leis e garantindo qualidade, pontualidade e zelo no atendimento à **CONTRATANTE**.
12.2.6. Não veicular publicidade ou qualquer outra informação relativa à **CONTRATANTE** ou aos serviços objeto deste contrato, sem prévia autorização da **CONTRATANTE**.

CLÁUSULA DÉCIMA TERCEIRA: DA GARANTIA

13.1. A garantia dos equipamentos, software, suporte técnico, instalação e configuração após seu pleno funcionamento será de 90 (noventa) dias e de responsabilidade da **CONTRATADA**, iniciando-se um dia útil após a emissão do Termo de Recebimento Definitivo.
13.2. Durante o período indicado acima, qualquer atividade relacionada ao funcionamento dos produtos, como manutenção evolutiva, preventiva e corretiva, estará incluída na garantia, sem nenhum ônus para o **CONTRATANTE**. Após este período, a garantia deverá ser realizada pelo fabricante do equipamento.
13.3. A garantia durante o período de 90 (noventa) dias deverá ser prestada pelo profissional indicado pela **CONTRATADA**.

CLÁUSULA DÉCIMA QUARTA: DISPOSIÇÕES FINAIS

14.1. O presente instrumento poderá ser modificado, através de Termos Aditivos, se de comum acordo entre as partes, vedada a alteração da natureza do objeto pactuado neste **CONTRATO**.
14.2. Fica eleito o Foro da Comarca de Belo Horizonte, Estado de Minas Gerais, que será o competente para dirimir dúvidas decorrentes da execução deste **CONTRATO**.
14.3. Caso a **CONTRATADA**, no decorrer da prestação dos serviços, demonstre inaptidão técnica, operacional ou administrativa, bem como quaisquer outras características que, no entendimento do **CONTRATANTE**, possa prejudicar, inviabilizar, retardar ou desvirtuar o objetivo pretendido, poderá o **CONTRATANTE** aplicar as penalidades previstas no presente contrato.
14.4. O não exercício, pelo **CONTRATANTE**, de qualquer dos direitos previstos neste contrato não constituirá renúncia ou novação, podendo tais direitos e prerrogativas ser por ela exercido a qualquer tempo.
14.5. Casos omissos e modificações serão resolvidos entre as partes através de termos aditivos, que farão parte integrante deste CONTRATO;
14.6. O **CONTRATANTE** poderá introduzir acréscimos ou supressões que se fizerem necessários, em até 50% (cinquenta por cento) do valor inicial do contrato, conforme lhe faculta o artigo 38 do Regulamento de Licitações e Contratos do Sescoop.
14.7. Os casos fortuitos ou de força maior serão excludentes de responsabilidade das partes, na forma do Código Civil Brasileiro.

Como alternativa à assinatura física do Instrumento, as Partes declaram e concordam que as assinaturas mencionadas poderão ser efetuadas em formato eletrônico, sendo a(s) respectiva(s) folha(s) de assinaturas documento integrante e inseparável deste Instrumento Contratual, sob pena de nulidade, declarando ainda e desde já, reconhecerem a veracidade, autenticidade e validade deste Instrumento e de seus termos, incluindo seus anexos, nos termos do art. 219 do Código Civil, por meio de certificados eletrônicos e digitais, nos termos do art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (“MP nº 2.200-2”) e da legislação vigente da autoridade certificadora ICP-Brasil.

E por estarem assim, justas e contratadas, assinam as partes o presente, na presença das testemunhas abaixo, que também o assinam.

Belo Horizonte, 18 de julho de 2024.

SESCOOP/MG

ALEXANDRE GATTI LAGES
SUPERINTENDENTE

ISABELA CHENNA PEREZ
GERENTE GERAL

PROCEDATA INFORMÁTICA LTDA

FERES MARON SALIM

TESTEMUNHAS

SAMUEL FABIANO BARBOSA SILVA

AMAURI ALVES DE ANDRADE

Protocolo de assinaturas

Documento

Nome do envelope: 110-2024 - CONTRATO - FORNECIMENTO SOFTWARE - PROCEDATA - 18-07
Autor: Amauri Alves de Andrade - amauri.andrade@sistemaocemg.coop.br
Status: Finalizado
HASH TOTVS: 95-60-14-F3-4C-49-48-1C-4A-F2-F2-08-E7-C8-93-19-5B-E2-8A-28
SHA256: 6b07e8ad1159bc671bbdfa140f4404079c80841175de5fc7806a77480e767728

Assinaturas

Nome: Carolina Pereira Carvalho - **CPF/CNPJ:** 119.326.266-62
E-mail: carolina.carvalho@sistemaocemg.coop.br - **Data:** 18/07/2024 10:50:36
Status: Assinado com certificado (A1/A3) para chancela jurídica
Tipo de Autenticação: Utilizando validação de código enviado por e-mail
Visualizado em: 18/07/2024 10:50:07 - **Leitura completa em:** 18/07/2024 10:50:19
IP: 201.86.118.234
Geolocalização: Indisponível ou compartilhamento não autorizado pelo assinante
Certificado Digital: CN=CAROLINA PEREIRA CARVALHO:11932626662, OU=16986332000127, OU=Presencial, OU=AR CERTDATA, OU=AC VALID RFB V5, OU=RFB e-CPF A3, OU=Secretaria da Receita Federal do Brasil - RFB, O=ICP-Brasil, C=BR

Nome: SAMUEL FABIANO BARBOSA SILVA -**CPF/CNPJ:** 092.346.566-95
E-mail: samuel.fabiano@sistemaocemg.coop.br - **Data:** 18/07/2024 14:01:50
Status: Assinado eletronicamente como testemunha
Tipo de Autenticação: Utilizando validação de código enviado por e-mail
Visualizado em: 18/07/2024 11:11:41 - **Leitura completa em:** 18/07/2024 14:01:30
IP: 201.86.118.234
Geolocalização: -19.9213666, -43.9341315

Nome: Amauri Alves de Andrade - **CPF/CNPJ:** 030.555.556-19 - **Cargo:** Analista de Licitações e Compras
E-mail: amauri.andrade@sistemaocemg.coop.br - **Data:** 18/07/2024 15:18:42
Status: Assinado eletronicamente como testemunha
Tipo de Autenticação: Utilizando login e senha, pessoal e intransferível
Visualizado em: 18/07/2024 15:18:27 - **Leitura completa em:** 18/07/2024 15:18:37
IP: 201.86.118.234
Geolocalização: -19.9275, -43.9278

Nome: Alexandre Gatti Lages - **CPF/CNPJ:** 005.361.356-22 - **Cargo:** Superintendente
E-mail: alexandre.gatti@sistemaocemg.coop.br - **Data:** 18/07/2024 17:43:20
Status: Assinado eletronicamente como responsável legal
Tipo de Autenticação: Utilizando login e senha, pessoal e intransferível
Visualizado em: 18/07/2024 17:43:09 - **Leitura completa em:** 18/07/2024 17:43:18
IP: 207.180.135.118
Geolocalização: Indisponível ou compartilhamento não autorizado pelo assinante

Nome: Isabela Chenna Pérez - **CPF/CNPJ:** 074.619.726-85 - **Cargo:** Gerente geral
E-mail: isabela.perez@sistemaocemg.coop.br - **Data:** 18/07/2024 22:22:21
Status: Assinado eletronicamente como responsável legal
Tipo de Autenticação: Utilizando login e senha, pessoal e intransferível
IP: Indisponível ou compartilhamento não autorizado pelo assinante
Geolocalização: Indisponível ou compartilhamento não autorizado pelo assinante

Nome: FERES MARON SALIM - **CPF/CNPJ:** 716.331.116-87
E-mail: feres.salim@procedata.com.br - **Data:** 23/07/2024 17:34:22
Status: Assinado eletronicamente como responsável legal
Tipo de Autenticação: Utilizando validação de código enviado por e-mail
Visualizado em: 23/07/2024 16:08:07 - **Leitura completa em:** 23/07/2024 16:08:27
IP: 177.182.168.92
Geolocalização: -19.9221, -43.9347

Autenticidade

Para verificar a autenticidade do documento, escaneie o QR Code ou acesse o link abaixo:

https://totvssign.totvs.app/webapptotvssign/#/verify/search?codigo=95-60-14-F3-4C-49-48-1C-4A-F2-F2-08-E7-C8-93-19-5B-E2-8A-28

HASH TOTVS: 95-60-14-F3-4C-49-48-1C-4A-F2-F2-08-E7-C8-93-19-5B-E2-8A-28