

**ENDEREÇO**

Ed. Florença em Palmas/TO  
Ed. Liberty Mall em Brasília/DF  
Ed. QS Tower em Goiânia/GO  
Av. José de Brito, 807 em Araguaína/TO

**CONTATO**

Diogo Borges  
(63) 3212-1952  
diogo.borges@crptecnologia.com.br

**ONLINE**

crptecnologia.com.br  
instagram.com/crptecnologia  
linkedin.com/crptecnologia

# PROPOSTA COMERCIAL

## PREGÃO PRESENCIAL Nº 14/2021

**AOS CUIDADOS**

**Celiene Gomes de Sousa** - Presidente da Comissão de  
Licitação do SENAR-AR/TO

**Pregão Presencial:** 14/2021

**Órgão Interessado:** SERVIÇO NACIONAL DE APRENDIZAGEM RURAL –  
ADMINISTRAÇÃO REGIONAL  
DO ESTADO DO TOCANTINS – SENAR-AR/TO

**VALIDADE**

Proposta Criada em: 25/11/2021

Validade da Proposta: 90 dias ✓

Proposta que faz a empresa **CRP Comercio de Equipamentos e Suprimentos de Informática LTDA-ME**, inscrita no CNPJ/CGC (MF) nº **20.998.285/0001-09** e inscrição estadual nº **29.460.367-0**, estabelecida no(a) Ed. Florença, 103 Norte (ACNO 11), Conj. 02, Rua NO 07, Lt 01 A23, 9º Andar, CEP 77.001-032, Palmas - TO, para atendimento a solicitação de proposta comercial para aquisição de produtos/serviço a seguir:



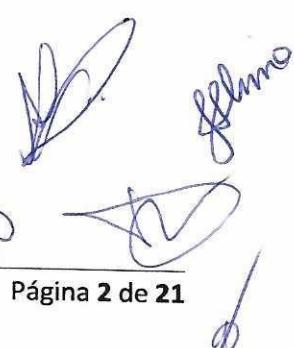
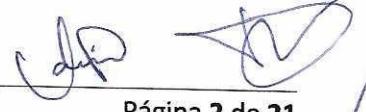
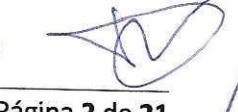
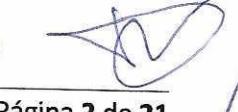


# INVESTIMENTO

## LOTE ÚNICO

		QTD	Unid.	Valor Unit. Mensal	Valor Total Anual
1	Serviços especializados em tecnologia da informação compreendendo o outsourcing nível 2 e 3. Os serviços abrangem os servidores de dados, redes cabeadas, redes sem fio, gestão de Active Directory, gestão de domínio, apoio e suporte nos sistemas internos próprios ou de terceiros utilizados pela contratante, exceto sistemas relacionados ao ambiente TOTVS.	01	Serviço	R\$ 7.000,00	R\$ 84.000,00
2	Serviços de Firewall composto por equipamentos e sistemas destinados à proteção da rede e controle do tráfego, contemplando o gerenciamento, suporte técnico do equipamento, monitoramento remoto e presencial, da solução de Firewall implantada.	01	Serviço	R\$ 3.000,00	R\$ 36.000,00
3	Serviços de Backup Profissional local com contingência e armazenamento em datacenter externo composto por equipamentos e sistemas, destinados à realização da proteção, armazenamento e recuperação de dados dos servidores e computadores com informações críticas, contemplando o gerenciamento, suporte técnico, monitoramento remoto e presencial da solução de Backup implantada com volume de no mínimo 3TB.	01	Serviço	R\$ 4.000,00	R\$ 48.000,00
<b>VALOR TOTAL MENSAL</b>				<b>R\$ 14.000,00</b>	
<b>VALOR TOTAL ANUAL</b>					<b>R\$ 168.000,00</b>
<b>Total por extenso R\$ 168.000,00 (cento e cinquenta e três mil e seiscentos reais)</b>					

- A Licitante DECLARA que no preço apresentado, estão incluídos todos os benefícios e os custos diretos e indiretos exigidos para prestação dos serviços, assim entendido, não somente as despesas diretas, com a aquisição de materiais e pagamento de mão-de-obra, como também as despesas indiretas, dentre elas: transporte de pessoal, alimentação, despesas financeiras, serviços de terceiros, aluguel e aquisição de máquinas, equipamentos, veículos, contribuições devidas à Previdência Social, encargos sociais e trabalhistas, impostos, taxas, emolumentos incidentes sobre o fornecimento, ou outras despesas, quaisquer que sejam as suas naturezas;
- A Licitante DECLARA estar ciente que deverá disponibilizar equipe de especialistas com os perfis técnicos adequados a prestação dos serviços a serem contratados;
- A Licitante DECLARA estar ciente da obrigatoriedade de comprovar quando da assinatura do contrato, as qualificações técnicas dos profissionais que executarão os serviços conforme estipulado no item 14 do Edital de Licitação.



Razão Social: **CRP Comercio de Equipamentos e Suprimentos de Informática LTDA-ME.**  
CGC (MF) nº: **20.998.285/0001-09** Insc. Estadual nº.: **29.460.367-0**

Endereço: **Quadra 103 Norte (ACNO 11), Rua NO 07, Conj. 02, Lt 01 A23, Ed. Florença 9º andar.**

Cidade: **Palmas** Estado: **TO** CEP: **77.001-032**

Fone/Fax: **(63) 3212-1952** E-mail: **comercial@crptecnologia.com.br**

Banco: **033 Santander Agência nº: 3932 Conta nº: 13004259-5**

**Representante legal p/ procuração para assinatura do contrato:**

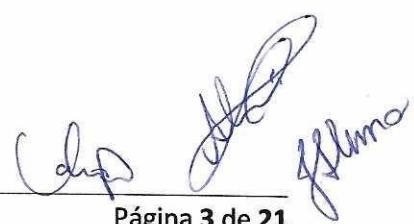
Nome: **Diogo Borges Oliveira** Cargo: **Analista Comercial**

RG: **803.030 SSP-TO** CPF: **013.544.021-11**

Naturalidade: **Céres-GO** Nacionalidade: **Brasileiro**

E-mail: **diogo.borges@crptecnologia.com.br** Telefone: **(63) 3212-1952**

  
**Diogo Borges Oliveira**  
Consultor de Negócios

  
Cássia, Henrique, Gleison

## ANEXO

### ACIONAMENTO DO SUPORTE N2 e N3

- **Atendimento:** De segunda a sexta-feira: das 08h00min às 18h00min, exceto feriados.
- **Canais de comunicação:**
  - **Telefone:** (63) 3212-1952
  - **E-mail:** [suporte@crptecnologia.com.br](mailto:suporte@crptecnologia.com.br)
  - **Ferramenta Web:** <http://suporte.crptecnologia.com.br/otrs/customer.pl>

### SOLUÇÕES (EQUIPAMENTOS/SOFTWARES/LICENÇAS) UTILIZADOS PARA REALIZAÇÃO DOS SERVIÇOS GERENCIADOS DE FIREWALL - ITEM 02

Part Number	Descrição	QTD
02-SSC-2821	SONICWALL TZ270	1
02-SSC-6745	ESSENTIAL PROTECTION SERVICE SUITE FOR TZ270 1YR	1
02-SSC-8184	SONICWALL ANALYTICS SOFTWARE (SYSLOG) FOR TZ270/TZ270W SERIES 1YR	1
01-SSC-5310	SONICWALL GLOBAL VPN CLIENT WINDOWS - 1 LICENSE (TOTAL = 7)	2
01-SSC-6111	FIREWALL SSL VPN 15 USER LICENSE (TOTAL = 16)	1

### SOLUÇÕES (EQUIPAMENTOS/SOFTWARES/LICENÇAS) UTILIZADOS PARA REALIZAÇÃO DOS SERVIÇOS GERENCIADOS DE BACKUP - ITEM 03

Part Number	Descrição	QTD
UBP-APP-TB-247	Software de Backup - RAPID RECOVERY BACKUP AND REPLICATION MSP	1
Dell T340	Servidor para Armazenamento do Backup - DellEMC PowerEdge T340	1
LINK-FO-30M	Link de Fibra Óptica de 30MEGA entre SENAR-TO e CRP	1

## 4 DAS ESPECIFICAÇÕES GERAIS DOS SERVIÇOS

### 4.1 Implantação das Soluções:

- 4.1.1 A CONTRANTE solicitará as implantações dos serviços adjudicados por meio de OS - Ordem de Serviço com o nome dos serviços a serem implantados;
- 4.1.2 Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados;
- 4.1.3 Todo pessoal e ferramental necessário para execução dos serviços de instalação e configuração incluindo equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da empresa CONTRATADA;
- 4.1.4 As soluções deverão ser instaladas e implementadas nas dependências da CONTRATADA por técnico(s) certificado(s) dos fabricantes das mesmas, sendo vedadas assistências técnicas ou terceirizados;
- 4.1.5 Todas as configurações e instalação da solução deverão ser realizadas em conformidade com a recomendação do fabricante, seguindo rigorosamente as boas práticas de implementação recomendadas;
- 4.1.6 Os equipamentos e sistemas que compõem os serviços deverão ser entregues e instalados na CONTRANTE. As fases da implantação dos serviços devem contemplar:
  - 4.1.6.1 **Planejamento:** nesta etapa a CONTRATADA deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano testes, a localização dos appliances na arquitetura da rede da CONTRANTE, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Deve-se considerar as janelas de manutenção da CONTRANTE, plano de rollback e o escopo definido. Os responsáveis técnicos da CONTRANTE acompanharão e aprovarão o planejamento.

- 4.1.6.1.1 O prazo máximo para implantação pela CONTRATADA será de 30 (trinta) dias corridos, contados a partir da data de assinatura do contrato.
- 4.1.6.2 **Implementação:** após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas, cumprimento dos prazos pactuados e o foco principal do projeto visando tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.
- 4.1.6.3 **Etapa de Testes:** todos os controles implantados para a ativação dos serviços gerenciados de segurança deverão ser testados a cada etapa pré-definida no planejamento. Além disso, o plano de rollback deverá garantir o retorno exequível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço.
- 4.1.6.4 **Homologação:** Após a conclusão dos testes, a solução deverá ser formalmente homologada pela CONTRANTE, com a finalidade de iniciar a monitoração, operação dos serviços e gerenciamento do ambiente, dentro dos níveis de serviço acordados.
  - 4.1.6.4.1 A CONTRANTE terá o prazo de 15 (quinze) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração dos serviços contratados, para emitir o relatório de homologação (aceite);
  - 4.1.6.4.2 O serviço será aceito se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características das soluções utilizadas, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações, comparadas aos itens deste Termo;

## 4.2 Serviços de Suporte Técnico

- 4.2.1 A CONTRATADA deverá prover os serviços objetos deste Termo de forma remota por meio da Central de Serviços e presencialmente, quando necessário;
- 4.2.2 A CONTRATADA deverá ter estrutura de suporte para atendimento presencial em Palmas – TO;
- 4.2.3 Os serviços de suporte técnico devem contemplar as seguintes ações e/ou premissas:
  - 4.2.3.1 Recepcionar via telefone ou e-mail, e registrar corretamente à abertura de qualquer chamado técnico referente à solução;
  - 4.2.3.2 Implantar e manter scripts de atendimento adequados às necessidades de suporte técnico do Contratante;
  - 4.2.3.3 Implantar e manter base de conhecimento adequada às necessidades de suporte técnico do Contratante;
  - 4.2.3.4 Solucionar problemas ou sanar dúvidas por telefone e/ou e-mail quanto aos questionamentos repassados pelo Contratante;
  - 4.2.3.5 Acionar equipes específicas da CONTRATADA para realizar a reposição antecipada de equipamentos defeituosos, quando for necessário;
  - 4.2.3.6 Realizar, mediante aviso e agendamento com o Contratante, atualização de softwares e firmwares dos produtos ofertados, quando disponibilizado pelo fabricante;
  - 4.2.3.7 Agendar visitas de manutenção corretiva com o Contratante, registrando chamados para este fim;
  - 4.2.3.8 Acompanhar os chamados desde sua abertura até seu encerramento, independente de existir ou não redirecionamento para outras equipes técnicas da própria CONTRATADA ou Fabricante;
- 4.2.4 Fazem parte do escopo do suporte técnico, durante sua vigência, os seguintes serviços:
  - 4.2.4.1 Disponibilizar atualizações de softwares e firmwares dos serviços/produtos ofertados sem qualquer tipo de ônus para o Contratante;
  - 4.2.4.2 Realizar visita local para manutenção preventiva dos produtos instalados na sede do Contratante em horário comercial, de segunda a sexta-feira das 08h00min às 18h00min, exceto feriados, sempre que necessário ou solicitado pelo Contratante;
  - 4.2.4.3 Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de 24h (vinte e quatro horas) após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição será ocorrer na sede do Contratante;
  - 4.2.4.4 A reposição antecipada deve ocorrer durante o período necessário em que o equipamento do Contratante estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;

- 4.2.4.5 A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente do Contratante;
- 4.2.4.6 Os serviços de suporte técnico devem estar disponíveis em horário comercial durante sua vigência, de segunda a sexta-feira das 08h00min às 18h00min;
- 4.2.4.7 Para os serviços de suporte técnicos, a CONTRATADA deverá possuir Central de Serviços disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados de segunda a sexta-feira, das 08h00min às 18h00min;
- 4.2.4.8 Caberá a Central de Serviços ser o contato único entre a CONTRATADA e a CONTRATANTE, registrando todas as solicitações e registros de ocorrência em sistema eletrônico específico para este, além de fornecer ao Contratante o número de identificação da ocorrência para acompanhamento. A Central de Serviços deverá disponibilizar software web para abertura de chamados e acompanhamento dos mesmos
- 4.2.5 O apoio ou suporte a sistemas internos ou terceirizados NÃO abrangem a NENHUMA solução do ambiente TOTVS, como RM, PROTHEUS ou outros sistemas dessa natureza.

#### **4.3 Atividades de gerenciamento:**

- 4.3.1 Gerais:
  - 4.3.1.1 Atualização de patches e novas versões de firmware nos equipamentos e softwares que compõem as soluções ofertadas, que forem disponibilizados na CONTRANTE;
  - 4.3.1.2 A CONTRANTE deverá possuir acesso de leitura aos equipamentos que forem utilizados para possibilitar o serviço, através de consoles de gerenciamento;
  - 4.3.1.3 O gerenciamento e suporte dos equipamentos remoto deverá ser feito via VPN;
- 4.3.2 Firewall:
  - 4.3.2.1 Realizar, via solução de Firewall especificada no item "Solução de Firewall" a proteção da rede, controle de acessos à internet e aplicativos, priorização de serviços, conforme políticas de segurança definidas juntamente com a CONTRATANTE;
  - 4.3.2.2 Inclusão/exclusão/alteração de regras, nos equipamentos Firewall UTM, com análise crítica a fim de garantir a gestão de mudanças no ambiente da CONTRANTE;
  - 4.3.2.3 Identificar brechas e vulnerabilidades na configuração de regras implantadas e propor, de forma contínua, melhorias na proteção do ambiente, sempre que identificado a necessidade;
- 4.3.3 Backup Profissional:
  - 4.3.3.1 Realizar, via solução profissional de backup especificada no item "Serviços de Backup Profissional" a proteção (backup) completa (sistema operacional, aplicativos instalados, configurações e dados), diário e/ou intervalos pré-determinados, automaticamente, dos servidores e computadores críticos elencados pela CONTRATANTE;
  - 4.3.3.2 Não haverá limitação de quantitativo de servidores e computadores a serem protegidos, a limitação se dará conforme volume de dados requisitado nos itens "Solução Profissional de Backup";
  - 4.3.3.3 Realizar a análise do ambiente atual da CONTRATANTE (identificando modo de operação) e efetuar ajustes no ambiente de backup caso necessário;
  - 4.3.3.4 Prestar todo o suporte técnico necessário para a perfeita execução do backup e/ou sua restauração e configuração;
  - 4.3.3.5 Realizar a recuperação (restauração) dos dados (da base de dados completa ou apenas arquivos específicos) sempre que demandado pela CONTRATANTE e sem custos adicionais;
  - 4.3.3.6 Trafegar os dados entre os servidores protegidos e o Datacenter externo (onde serão replicados o backup), com padrões de Segurança (ex: Criptografia, etc.);
  - 4.3.3.7 Propor, de forma contínua, melhorias no sistema de backup, sempre que identificado a necessidade;

#### **4.4 Acordo de Nível de Serviço (ANS):**

- 4.4.1 Os tempos máximos de atendimento especificados nas tabelas a seguir, sob pena de multa;
- 4.4.2 Em casos emergenciais, quando houver a paralisação nas atividades do negócio ou uma demanda de nível superior, a CONTRANTE poderá abrir chamados emergenciais, com o ANS diferenciado, cujo tempo de resposta para todas as atividades listadas na tabela acima passam a ter tempo máximo de resposta

de 60 minutos. A CONTRANTE deverá designar até 4 (quatro) pessoas que poderão abrir chamados emergenciais.

#### 4.4.3 Chamados de Firewall UTM:

Atividade	Tempo de Resposta Máximo
Alteração e inclusão de regras.	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Alteração de configurações.	180 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Atualização (implementação de patches e fixes).	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pela CONTRANTE.
Início de atuação remota para resolução de problemas.	180 minutos após abertura de chamado
Implementação de novos serviços ou dispositivos.	24 horas após abertura de chamado

**Tabela 1 - ANS para chamados de Firewall UTM**

#### 4.4.4 Chamados de Backup Profissional:

Atividade	Tempo de Resposta Máximo
Proteção de um novo servidor/computador.	48 horas após abertura de chamado.
Alteração das políticas atuais de backup.	8 horas após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Atualização (implementação de patches e fixes).	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pela CONTRANTE.
Início de atuação remota para resolução de problemas.	180 minutos após abertura de chamado
Recuperação de dados e/ou servidor/computador por completo.	3 horas após abertura de chamado, exceto quando for necessária uma janela de manutenção.

**Tabela 2 - ANS para chamados de Backup Profissional**

#### 4.5 Serviços de monitoramento remoto:

##### 4.5.1 Gerais:

- 4.5.1.1 A CONTRATADA deverá monitorar remotamente os equipamentos de Firewall que forem ofertados. Os serviços deverão ser prestados remotamente, a partir de um Centro de Operação de Segurança da CONTRATADA, estritamente de acordo com as especificações deste documento;
- 4.5.1.2 Os serviços de monitoramento remoto deverão ser realizados pela CONTRATADA, na modalidade, 8h por dia, 5 dias por semana de segunda-feira a sexta-feira das 8h às 18h, exceto feriados;
- 4.5.1.3 A CONTRATADA deverá monitorar remotamente os eventos abaixo relacionados e alertar a CONTRANTE para as providências cabíveis;

##### 4.5.2 Firewall:

- 4.5.2.1 Intrusões detectadas pelos módulos de IPS e antivírus do equipamento de Firewall ofertado;
- 4.5.2.2 Indisponibilidade do cluster de Firewall;
- 4.5.2.3 Indisponibilidade de VPN;
- 4.5.2.4 Indisponibilidade dos links de Internet;
- 4.5.2.5 Sobrecarga de processamento;
- 4.5.2.6 A CONTRATADA deverá disponibilizar, mensalmente, até o 5º dia útil do mês posterior à prestação de serviços, através de e-mail ou via impressa, os seguintes relatórios de utilização dos últimos 30 (trinta) dias:



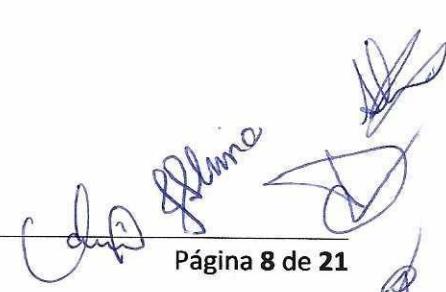
- 4.5.2.6.1 Usuários com maior atividade permitida (pelo endereço IP/nome do usuário);
- 4.5.2.6.2 Domínios mais acessados;
- 4.5.2.6.3 Categorias de site mais acessadas;
- 4.5.2.6.4 Aplicações mais acessadas;
- 4.5.2.6.5 Categorias de aplicações mais acessadas;
- 4.5.2.6.6 Aplicações bloqueadas;
- 4.5.2.6.7 Categorias de aplicações mais bloqueadas;
- 4.5.2.6.8 Protocolos IP com maior atividade (entrada e saída);
- 4.5.2.6.9 Relatório de malwares detectados;
- 4.5.2.6.10 Relatório de tentativas de intrusão.

**4.5.3 Backup Profissional:**

- 4.5.3.1 Gerenciar e monitorar o backup diário de dados, alertando em casos de falhas, pouco espaço em disco ou erros de qualquer natureza e propor e/ou realizar a imediata correção;
- 4.5.3.2 A CONTRATADA deverá disponibilizar, mensalmente, até o 5º dia útil do mês posterior à prestação de serviços, através de e-mail ou via impressa, os seguintes relatórios de utilização dos últimos 30 (trinta) dias:
  - 4.5.3.2.1 Status de trabalhos bem-sucedidos, trabalhos com falha e trabalhos com erros;
  - 4.5.3.2.2 Máquinas protegidas, máquinas replicadas e pontos de restauração disponíveis;
  - 4.5.3.2.3 Status do repositório, contendo volume consumido e volume livre;

**4.6 Regime de Atendimento:**

- 4.6.1 De segunda a sexta-feira: das 08h00min às 18h00min, exceto feriados.





## 5 ESPECIFICAÇÕES DETALHADAS DOS SERVIÇOS

### 5.1 Requisitos Gerais:

- 5.1.1 Todos os equipamentos, produtos, peças ou softwares ofertados para composição dos serviços solicitados, deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante e cobertos por garantia do fabricante pelo período de 12 (doze) meses;
- 5.1.2 Todos os softwares deverão ser fornecidos em sua versão mais atual do fabricante, devendo constar na proposta comercial o seu PART NUMBER e/ou versão para efeito de comprovação;
- 5.1.3 É obrigatória a comprovação técnica de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do termo de referência sem a devida comprovação acarretará na desclassificação da empresa proponente;
- 5.1.4 Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s) para composição dos serviços, assim como informar marca e modelo do equipamento. O simples fato de "COPIAR" e "COLAR" o descritivo contido no edital não será caracterizado como descritivo da proposta;
- 5.1.5 Deverão ser informados todos os componentes relevantes da solução proposta com seus respectivos códigos do fabricante (marca, modelo, fabricante e part numbers), descrição e quantidades;
- 5.1.6 O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança;
- 5.1.7 Serão aceitos como documentos de comprovações técnicas:
  - 5.1.7.1 Documentos emitidos pelo fabricante dos produtos, na língua portuguesa ou inglesa, de preferência disponíveis na Internet (indicar o link onde podem ser obtidos). Declarações do fabricante somente serão aceitas se utilizadas em conjunto com documentos de comprovação como manuais, páginas da Internet, telas do produto ou outros documentos técnicos, que contenham o requisito solicitado;
  - 5.1.7.2 Declarações de conformidade com o termo, no caso do item de comprovação referir-se apenas a serviço a ser prestado pelo proponente;

### 5.2 Serviço de Suporte em TI Nível 2 e Nível 3

- 5.2.1 O Serviço de Terceiro Nível prestado pela CONTRATADA abrangerá apenas os usuários internos do Contratante;
- 5.2.2 O Serviço de Atendimento e Suporte Técnico de 2º e 3º Nível atuará na resolução de incidentes e requisições de serviços escalados pelo Serviço de Atendimento e Suporte Técnico de 1º Nível, além de elaborar e gerir procedimentos, scripts e itens da base de conhecimento sobre erros conhecidos, atuando em incidentes ou solicitações de maior complexidade e aqueles que envolvem usuários especiais;
- 5.2.3 A equipe alocada neste serviço buscará prevenir a ocorrência de problema se seus incidentes resultantes eliminarem incidentes recorrentes correlacionando-os e identificando a causa raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos;
- 5.2.4 Os chamados deverão, preferencialmente, ser atendidos remotamente, desde que a natureza do problema assim o permita, e o usuário concorde e autorize;
- 5.2.5 Todos os atendimentos realizados pela equipe de Atendimento a Usuários, que gerem alguma alteração nos componentes que foram objeto de suporte, deverão ser documentados para fins de atualização da Base de Conhecimento e documentação do sistema. Quando necessário, a equipe técnica do Contratante poderá ser acionada para dar suporte à atividade de manutenção da Base de Conhecimento;
- 5.2.6 Principais atividades a serem executadas
  - 5.2.6.1 Prestar suporte remoto, de terceiro nível, aos usuários internos de TI do Contratante, no atendimento de requisições de serviço e resolução de incidentes ou problemas não



resolvidos pelo Serviço de Atendimento e suporte Técnico de 2º Nível, respeitando os níveis de serviço acordados.

- 5.2.6.2 A prestação dos serviços de suporte de ambiente em 3<sup>a</sup> nível será para prestação dos serviços de manutenção da operação da infraestrutura de TI do órgão, tendo por objetivo principal:
- 5.2.6.3 Administrar sistemas operacionais, redes (cabeadas e sem fio), segurança, colaboração, armazenamento, backup e virtualização;
- 5.2.6.4 Analisar pró-ativamente a infraestrutura do ambiente tecnológico do órgão Contratante;
- 5.2.6.5 Corrigir erros detectados que não puderam ser resolvidos pelos demais níveis;
- 5.2.6.6 Atender os chamados de sustentação de infraestrutura;
- 5.2.6.7 Encaminhar chamados resolvidos para o 1º nível efetuar o encerramento;
- 5.2.6.8 Elaborar relatórios sobre o ambiente de rede, incluindo relatório de erros, de desempenho e de atividades;
- 5.2.6.9 Elaborar plano de trabalho para atividades demandas por solicitação de serviço;
- 5.2.6.10 Instalar, desinstalar, atualizar, configurar, customizar e parametrizar softwares de alta complexidade;
- 5.2.6.11 Monitorar e garantir a disponibilidade acordada para os servidores e serviços de rede (cabeadas e sem fio) do órgão Contratante;
- 5.2.6.12 Configurar switches ethernet e pontos de acesso de redes sem fio;
- 5.2.6.13 Instalar e desinstalar ativos de redes no Datacenter e nas salas de comunicação do edifício sede do órgão Contratante;
- 5.2.6.14 Elaborar relatórios sobre o ambiente de infraestrutura, incluindo relatório de incidente, de desempenho e de atividades, quando necessário;
- 5.2.6.15 Monitorar disponibilidade dos serviços críticos;
- 5.2.6.16 Administrar a capacidade dos servidores físicos e virtuais;
- 5.2.6.17 Realizar manutenção preventiva dos servidores físicos e virtuais;
- 5.2.6.18 Criar grupos e administrar perfis de acesso;
- 5.2.6.19 Criar e executar consultas personalizadas quando solicitado;
- 5.2.6.20 Garantir a integridade, disponibilidade e confidencialidade dos serviços;
- 5.2.6.21 Elaborar e revisar, tecnicamente, documentos operacionais, gerenciais e de desempenho;
- 5.2.6.22 Criar ou atualizar os templates para a criação dos servidores virtuais;
- 5.2.6.23 Atuar no gerenciamento da plataforma Windows Server e Linux e na administração de domínio de rede;
- 5.2.6.24 Criar e manter políticas de grupos;
- 5.2.6.25 Implantar e gerenciar os serviços do Windows.
- 5.2.6.26 Atuar na operação de servidores de aplicação Internet Information Services – IIS;
- 5.2.6.27 Atuar na operação de servidores de aplicação Apache, JBoss e Tomcat;
- 5.2.6.28 Instalar, configurar e gerenciar a solução de virtualização VMware;
- 5.2.6.29 Instalar e configurar novos servidores e appliances, físicos e virtuais;
- 5.2.6.30 Auxiliar no desenvolvimento, na aplicação e fiscalização das políticas, normas, padrões e procedimentos de segurança institucionais e backup;
- 5.2.6.31 Monitorar a rede de modo a identificar programas, ou atitudes maliciosas ou atividades suspeitas que possam comprometer a segurança institucional;
- 5.2.6.32 Analisar links de Internet disponibilizados pelo Contratante;
- 5.2.6.33 Acompanhar as migrações tecnológicas, novas instalações e outras demandas junto à área responsável ou fornecedores;
- 5.2.6.34 Prospectar novas tecnologias para o aperfeiçoamento das soluções existentes;
- 5.2.6.35 Analisar novas soluções propostas pelo cliente, emitindo nota técnica;
- 5.2.6.36 Analisar e buscar correções para as falhas, erros e alertas;
- 5.2.6.37 Identificar, relatar e aplicar atualizações e correções tecnológicas que possam comprometer a segurança institucional;
- 5.2.6.38 Criar scripts de automação e de monitoração dos servidores;
- 5.2.6.39 Gerenciar softwares, firmwares e equipamentos de segurança, backup, virtualização, rede, storage e sistemas operacionais e web, fornecidos pelo cliente;
- 5.2.6.40 Elaborar relatório de vulnerabilidade das aplicações e sistemas corporativos;
- 5.2.6.41 Executar requisições de mudanças autorizadas pela área demandante, conforme procedimento;
- 5.2.6.42 Criar ou revisar documentação técnica (procedimentos e manuais) das atividades realizadas;
- 5.2.6.43 Revisar as configurações dos servidores;

- 5.2.6.44 Realizar atividades relacionadas às rotinas de backup tais como, monitoramento, disponibilização, controle, transferência, armazenamento, liberação e restore das mídias;
- 5.2.6.45 Aplicar patches ou mudança de versão em servidores e clientes;
- 5.2.6.46 Monitorar ininterruptamente servidores e serviços através de ferramentas adequadas;
- 5.2.6.47 Apoiar as atividades das demais áreas em assuntos relacionados à infraestrutura e sustentação;
- 5.2.6.48 Testar comunicações e outras ferramentas que fizerem necessárias para execução da atividade;
- 5.2.6.49 Enviar relatório com eventos de monitoração remota;
- 5.2.6.50 Viabilizar a transmissão de reuniões e eventos através de soluções de vídeo streaming e videoconferência;
- 5.2.6.51 Analisar desempenho do ambiente de infraestrutura;
- 5.2.6.52 Instalar, desinstalar, montar, configurar e remanejar os equipamentos do datacenter;
- 5.2.6.53 Administrar serviços de mensagens;
- 5.2.6.54 Implantar soluções para monitoramento de serviços e servidores;
- 5.2.6.55 Criar escopos no DHCP e zonas no DNS;
- 5.2.6.56 Criar e manter certificados para sites e aplicações web;
- 5.2.6.57 Inventariar softwares e hardwares da infraestrutura tecnológica;
- 5.2.6.58 Gerenciar e sincronizar as configurações dos servidores físicos e virtuais;
- 5.2.6.59 Conferir, executar e criar scripts para o suporte e infraestrutura tecnológica e service desk;
- 5.2.6.60 Efetuar a manutenção de soluções de contingência nos ambientes tecnológicos de infraestrutura;
- 5.2.6.61 Realizar análise de viabilidade e propor soluções para demandas ou problemas;
- 5.2.6.62 Automatizar envio de relatórios, comandos de manutenção e processos repetitivos;
  
- 5.2.7 **Requisitos de qualificação de profissional para execução do serviço**
- 5.2.7.1 Formação completa em nível superior na área de Tecnologia da Informação, reconhecido pelo MEC, comprovada através de diploma ou certificado de conclusão de curso ou documento equivalente;
- 5.2.7.2 Experiência de, no mínimo, 5 (cinco) anos na área de infraestrutura de TI envolvendo Arquitetura de Computadores;
- 5.2.7.3 Conhecimento em Sistemas Operacionais (Windows, Unix, GNU/Linux);
- 5.2.7.4 Cultura do Desenvolvimento / Operação: Conhecimento de programação e domínio dos Sistemas operacionais e demais aspectos de uma infraestrutura de TI;
- 5.2.7.5 Segurança Computacional;
- 5.2.7.6 Automação de Tarefas;
- 5.2.7.7 Análise de logs;
- 5.2.7.8 Monitoramento de Sistemas e Serviços em Redes;

### 5.3 Solução de Firewall

- 5.3.1 **Características Gerais:**
  - 5.3.1.1 Devem ser fornecidas todas as licenças necessárias para o funcionamento das funcionalidades de Filtro de Conteúdo Web, IPS, Gateway Antivírus e Controle de Aplicações.
  - 5.3.1.2 A solução de Firewall deverá ser baseada em software + appliance, no qual o appliance deve possuir as seguintes características:
    - 5.3.1.2.1 Ser compatível para montagem em rack de 19" ou mesa;
    - 5.3.1.2.2 Possuir fonte de alimentação interna ou externa com operação automática entre 110/220V;
    - 5.3.1.2.3 Deve possuir no mínimo 08 (oito) interfaces 10/100/1000Base-TX, todas operando em modo auto-sense e em modo half/full duplex, com inversão automática de polaridade;
    - 5.3.1.2.4 Possuir porta console (serial ou RJ45) para possíveis manutenções no produto. Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

- 5.3.1.2.5 Possuir memória flash com capacidade suficiente para armazenamento do sistema operacional do firewall. Não serão aceitos Sistemas Operacionais do Tipo “Harderizado”;
- 5.3.1.2.6 O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, de um firewall não sendo baseado em plataforma X86 ou equivalente;
- 5.3.1.3 Não serão permitidas soluções baseadas em sistemas operacionais abertos como Free BSD, Debian ou mesmo Linux;
- 5.3.1.4 A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP;
- 5.3.1.5 As 08 (oito) interfaces de rede do appliance deverão ser configuráveis pelo administrador do firewall para atender os segmentos de segurança e rede para:
- 5.3.1.5.1 Segmento WAN, ou externo;
  - 5.3.1.5.2 Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema;
  - 5.3.1.5.3 Segmento LAN ou rede interna;
  - 5.3.1.5.4 Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada);
  - 5.3.1.5.5 Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade;
  - 5.3.1.5.6 Segmento ou Zona dedicada para controle de dispositivos Wireless dedicado com controle e configuração destes dispositivos;
- 5.3.1.6 Suportar no mínimo 50 (cinquenta) VLANs de interface (802.1q) suportando a definição de seus endereços IP através da interface gráfica;
- 5.3.1.7 O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL onde o mesmo deverá ser descriptografado de forma transparente a aplicação, verificado possíveis ameaças e então re-criptografado enviado juntamente ao seu destino caso este não contenha ameaças ou vulnerabilidades. O recurso poderá ser fornecido através de uma licença adicional/opcional ao equipamento;
- 5.3.1.8 Não possuir limitação de segmentos de rede a serem protegidos;
- 5.3.1.9 Suportar usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Esta comprovação poderá ser exigida em testes sob o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens;
- 5.3.1.10 Suportar usuários autenticados através de sistema denominado como “Captive Portal” interceptando para autenticação os usuários que não possuam seus dispositivos associados ao domínio da organização;
- 5.3.1.11 Deve implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 (três) servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;
- 5.3.1.12 Possibilitar o controle do tráfego para os protocolos TCP, UDP, ICMP e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;
- 5.3.1.13 O appliance deve permitir a utilização de políticas de Antivírus, Anti-Spyware e IPS/IDP e filtro de Conteúdo segmentos (todos os serviços devem ser suportados no mesmo segmento) ou por zonas de acesso ou VLANS;
- 5.3.1.14 Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/Anti-Spyware;
- 5.3.1.15 Possibilitar o controle do tráfego para os protocolos GRE, H323 Full v1-5, suporte à tecnologia a gatekeeper, SIP e IGMP baseados nos endereços origem e destino da comunicação;
- 5.3.1.16 Controle e gerenciamento de banda para a tecnologia VoIP sobre diferentes segmentos de rede/seurança com inspeção profunda de segurança sobre este serviço;
- 5.3.1.17 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;
- 5.3.1.18 Prover mecanismos de proteção contra-ataques baseados em “DNS Rebinding” protegendo contra códigos embutidos em páginas Web com base em JavaScript, Flash e base Java com



- "malwares". O recurso deverá prevenir ataques e analises aos seguintes endereços: Node-local address 127.0.0.1, Link-local address 169.254.0.0/24, Multicast address 224.0.0.0/24 e host que pertence há alguma das sub-nets conectadas a: LAN, DMZ ou WLAN;
- 5.3.1.19 Prover servidor DHCP Interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;
  - 5.3.1.20 Prover a capacidade de encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como IP Helper suportando os protocolos e portas: Time service—UDP porta 37, DNS—UDP porta 53, DHCP—UDP portas 67 e 68, Net-Bios DNS—UDP porta 137, Net-Bios Datagram—UDP porta 138, Wake On LAN—UDP porta 7 e 9, mDNS—UDP porta 535;
  - 5.3.1.21 Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, SIP, 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;
  - 5.3.1.22 Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;
  - 5.3.1.23 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como FTP, HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores Windows 2012/2016/2019 com AD;
- 5.3.2 Características Anti-Malware**
- 5.3.2.1 O firewall deverá possuir a função de Gateway Anti-Malware, no qual deverá suportar análise de pelo menos os protocolos, CIFS, NETBIOS, HTTP, FTP, IMAP, SMTP e POP3;
  - 5.3.2.2 Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados;
  - 5.3.2.3 A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;
  - 5.3.2.4 Devem ser fornecidas todas as atualizações da base de assinaturas de Anti-Malware de Gateway, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item;
- 5.3.3 Características IPS / IDS**
- 5.3.3.1 Possuir Mecanismo de IPS / IDS, com suporte a pelo menos 2.500 (duas mil e quinhentas) assinaturas de ataques, aplicações ou serviços, completamente integrados ao Firewall;
  - 5.3.3.2 Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados;
  - 5.3.3.3 A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;
  - 5.3.3.4 Devem ser fornecidas todas as atualizações para a base de assinaturas do IPS, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item;
- 5.3.4 Características de VPN**
- 5.3.4.1 Suportar padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;
  - 5.3.4.2 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;
  - 5.3.4.3 Suportar túneis VPN IPSEC do tipo site-to-site;
  - 5.3.4.4 Suportar túneis VPN IPSEC do tipo client-to-site;
  - 5.3.4.5 Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication;
  - 5.3.4.6 Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário;
  - 5.3.4.7 Deve suportar conexões clientes do tipo SSL VPN (VPNClient);

**5.3.5 Características de NAT**

- 5.3.5.1 Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;
- 5.3.5.2 Permitir, sobre o recurso de NAT, o balanceamento interno de servidores e suas aplicações sem a necessidade de inserção de um equipamento como switches de que atuam entre as camadas 4 (quatro) e 7 (sete) do modelo ISO/OSI;
- 5.3.5.3 Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino;
- 5.3.5.4 Possuir mecanismo que permita conversão de portas (PAT);

**5.3.6 Características de QoS**

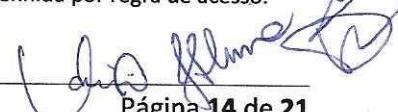
- 5.3.6.1 Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;
- 5.3.6.2 Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);
- 5.3.6.3 Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

**5.3.7 Características de Performance:**

- 5.3.7.1 A performance de Firewall SPI (Stateful Packet Inspection) deve ser de no mínimo 2 Gbps;
- 5.3.7.2 Deve suportar, em modo firewall, no mínimo 700.000 (setecentas mil) de conexões concorrentes;
- 5.3.7.3 Deve suportar, em modo DPI (análise profunda de pacotes com os serviços IPS, Anti-Malware e Controle de Aplicações) no mínimo 140.000 (cento e quarenta) conexões concorrentes;
- 5.3.7.4 Deve suportar no mínimo 5.000 (cinco mil) novas conexões por segundo;
- 5.3.7.5 Performance de todos os serviços ativos (Gateway Antivírus, Gateway Anti Spyware, IDS, IPS, Controle de Aplicações e Filtro de Conteúdo) deverá ser de no mínimo 500 Mbps;
- 5.3.7.6 A performance para inspeção de Anti-Malware integrado no mesmo appliance deve ser de no mínimo 700 Mbps;
- 5.3.7.7 A performance de IPS deve ser de no mínimo 1 Gbps;
- 5.3.7.8 A performance mínima para a funcionalidade de análise de tráfegos criptografados HTTPS/SSL deverá ser de 300 Mbps;
- 5.3.7.9 A performance de VPN IPSEC (3DES & AES 256) deverá ser de no mínimo 700 Mbps;
- 5.3.7.10 Deve suportar no mínimo 50 (cinqüenta) túneis VPN IPSEC do tipo site-to-site já licenciadas;
- 5.3.7.11 Deve suportar no mínimo 100 (cem) túneis VPN IPSEC do tipo client-to-site e, caso houver licenciamento adicional para esta funcionalidade, o equipamento deve ser ofertado com no mínimo 7 (sete) túneis já licenciados, suportando no futuro a utilização de mais túneis, baseado na aquisição de licenciamento adicional;
- 5.3.7.12 Deve suportar no mínimo 50 (cinquenta) conexões clientes do tipo SSL VPN (VPNClient) e, caso houver licenciamento adicional para esta funcionalidade, o equipamento deve ser ofertado com no mínimo 16 (dezesseis) licenças/conexões;
- 5.3.7.13 Suportar no mínimo 50 (cinqüenta) VLANs de interface (802.1q) suportando a definição de seus endereços IP através da interface gráfica;
- 5.3.7.14 Deve suportar no mínimo 500 (quinquinhos) usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança.

**5.3.8 Outras Características**

- 5.3.8.1 Possuir controle de número máximo de sessões TCP, prevenindo a exaustão de recursos do appliance e permitindo a definição de um percentual do número total de sessões disponíveis que podem ser utilizadas para uma determinada conexão definida por regra de acesso.



- 5.3.8.2 Possuir suporte ao protocolo SNMP versões 2 e 3;
- 5.3.9 **Características de Roteamento**
  - 5.3.9.1 Possuir roteamento RIP e OSPF, com configuração pela interface gráfica;
  - 5.3.9.2 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.
  - 5.3.9.3 Permitir que seja criado políticas de roteamentos estáticos 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.
  - 5.3.9.4 Possibilitar o roteamento de tráfego IGMP versão 3 em suas interfaces e zonas de segurança.
- 5.3.10 **Características de Gerenciamento**
  - 5.3.10.1 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
  - 5.3.10.2 Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reiniciar o sistema;
  - 5.3.10.3 Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
  - 5.3.10.4 Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas;
  - 5.3.10.5 Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall;
  - 5.3.10.6 Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
  - 5.3.10.7 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;
  - 5.3.10.8 Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;
- 5.3.11 **Características de Alta Disponibilidade**
  - 5.3.11.1 Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Ativo e/ou Ativo/Standby, com as implementações de Fail Over e Load Balance, sendo que na implementação de Load Balance o estado das conexões e sessões TCP e UDP deve ser replicado sem restrições de serviços como, por exemplo, tráfego multicast;
  - 5.3.11.2 Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;
  - 5.3.11.3 O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge;
- 5.3.12 **Autenticação**
  - 5.3.12.1 Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores NT e Unix, de forma simultânea;
  - 5.3.12.2 Permitir a utilização de LDAP, AD e RADIUS;
  - 5.3.12.3 Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;
  - 5.3.12.4 Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
  - 5.3.12.5 Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, XP e Windows 7, Windows 8 e 8.1, 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;

5.3.12.6 Possuir perfis de acesso hierárquicos;

5.3.12.7 Permitir a restrição de atribuição de perfil de acesso à usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.

**5.3.13 Filtro de Conteúdo Web**

5.3.13.1 Possuir módulo integrado ao mesmo Firewall DPI (Deep Packet Inspection) para classificação de páginas web com no mínimo 56 categorias distintas pré-definidas, com mecanismo de atualização automática;

5.3.13.2 Das categorias pré-definidas, devem existir pelo menos as seguintes: violência, nudismo, roupas íntimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar, hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting;

5.3.13.3 Controle de conteúdo filtrado por categorias de filtragem com base de dados continuamente atualizada e extensível;

5.3.13.4 Capacidade de submissão instantânea de novos sites e palavras chaves;

5.3.13.5 Permitir a classificação dinâmica de sites Web, URLs e domínios;

5.3.13.6 O administrador de política de segurança poderá definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

5.3.13.7 O administrador de política de segurança poderá personalizar quais zonas de segurança, em cada um dos firewalls da rede, terão aplicadas as políticas de filtragem de WEB, e de maneira centralizada;

5.3.13.8 O administrador poderá adicionar filtros por palavra-chave de modo específico e individual em cada um dos firewalls da rede, de forma centralizada;

5.3.13.9 A política de Filtros de conteúdo deverá ser baseada em horário do dia e dia da semana;

5.3.13.10 Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

5.3.13.11 Possibilitar a filtragem da linguagem Javascript e de applets Java e Active-X em páginas WWW, para o protocolo HTTP;

5.3.13.12 Deverá ser fornecida todas as atualizações de software assim como a atualização da base de conhecimento (URLs categorizadas), sem custo adicional, por um período de igual ou superior ao período de garantia e suporte solicitado para este item;

**5.3.14 Controle de aplicações**

5.3.14.1 A solução deve possuir a capacidade de identificar pelo menos 1.500 (mil e quinhentas) aplicações para controle, bloqueio e agendamento deste recurso por usuário e grupo de usuário;

5.3.14.2 Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos;

5.3.14.3 Devem ser aplicados por usuário e por grupo;

5.3.14.4 Associado suas ações políticas de horários e dias da semana;

5.3.14.5 Permitir ser associados a endereçamento IP baseados em sub-redes;

5.3.14.6 Permitir a restrição de arquivos por sua extensão e bloqueio de anexos através de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime;

5.3.14.7 Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa;

5.3.14.8 Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada;

5.3.14.9 Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada

*[Handwritten signatures]*

perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

- 5.3.14.10 Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 HTTP, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

**5.3.15 Log**

- 5.3.15.1 Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 5.3.15.2 Prover mecanismo de consulta às informações registradas integrado à interface de administração;
- 5.3.15.3 Possibilitar o armazenamento de seus registros (log e/ou eventos) na mesma plataforma de gerenciamento e descrito no item "Software para Gerenciamento de Logs e Relatórios";
- 5.3.15.4 Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica;
- 5.3.15.5 Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado;
- 5.3.15.6 Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;
- 5.3.15.7 Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;
- 5.3.15.8 Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;
- 5.3.15.9 Possui suporte a log via syslog;

**5.3.16 Software para Gerenciamento de Logs e Relatórios**

- 5.3.16.1 A solução de Firewall a ser entregue, deverá possuir módulo de relatórios, podendo este ser oferecida em appliance separado do próprio fabricante da solução de segurança para esta finalidade ou ambiente virtualizado, também do próprio fabricante, rodando sobre sistemas como VMware ESx ou ESXi, ou ainda em tecnologias baseadas em sistemas operacionais que tenham como base a plataforma Windows.
- 5.3.16.2 O produto deverá suportar a interação as bases de dados Microsoft SQL 2000, 2005, 2008 e MYSQL 5.0.
- 5.3.16.3 O appliance poderá possuir no máximo 1U de altura caso a solução seja fornecida nesta plataforma.
- 5.3.16.4 Possuir no mínimo duas interfaces Giga Bit Ethernet.
- 5.3.16.5 Caso a solução seja fornecida em appliance, possuir uma interface serial para possíveis manutenções e acesso a console.
- 5.3.16.6 Caso a solução seja fornecida em appliance, o armazenamento total em disco (SATA) deverá ser de no mínimo 2.25 TB, operando em modo RAID 5. Estes discos poderão ainda ser substituídos pela contratante / contratada sem a paralisação parcial ou total do sistema.
- 5.3.16.7 Deve fornecer gerência remota, com interface gráfica nativa, através do aplicativo ActiveX ou Java.
- 5.3.16.8 Deve fornecer interface gráfica para no mínimo 10 (dez) usuários simultâneos;
- 5.3.16.9 A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos firewalls sem a necessidade de se executar várias interfaces;
- 5.3.16.10 Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;
- 5.3.16.11 Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML, PDF e CSV: máquinas mais acessadas, serviços mais utilizados, usuários que mais

utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail, detecção de intrusos, intrusos bloqueados e alvos, para vírus e spywares bloqueados, alvos e detectados;

5.3.16.12 Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);

**5.3.17 Documentação Técnica, Certificações e Compatibilidade**

- 5.3.17.1 A solução deverá possuir certificações ICSA para Firewall e Antivírus;
- 5.3.17.2 O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no "Security Value Map" acima de 90% (noventa por cento) da avaliação de segurança efetiva;
- 5.3.17.3 O Fabricante deve comprovar participação no MAPP da Microsoft;
- 5.3.17.4 Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;

**5.4 Solução Profissional de Backup em Disco**

**5.4.1 Características Gerais:**

- 5.4.1.1 Realizar via solução profissional de backup especificada a proteção (backup) completa (sistema operacional, aplicativos instalados, configurações e dados), diário e/ou intervalos pré-determinados, automaticamente, dos servidores e computadores críticos elencados pela CONTRATANTE;
- 5.4.1.2 Armazenar 01 (uma) cópia de todo backup de dados em appliance/servidor de backup fornecido pela CONTRATADA, instalado localmente no ambiente da CONTRATENTE e realizar 01 (uma) cópia, no mínimo uma vez ao dia, em Datacenter externo seguro (sob responsabilidade da CONTRATADA);
- 5.4.1.3 A solução deve ter capacidade de armazenamento suficiente proteção de no mínimo 3TB (três terabytes) de dados "front-end", ou seja, será considerado o volume a ser protegido e não o espaço necessário para armazenar o backup;
- 5.4.1.4 Deverá possibilitar configuração de política de backup para realizar snapshots com frequência de 10 em 10 minutos, podendo essa frequência ser customizável para cada servidor protegido, conforme interesse da CONTRATANTE;
- 5.4.1.5 Deverá reter os dados protegidos pelo período mínimo de 30 (trinta) dias sem sobrescrever-los, e o espaço adicional necessário para esta retenção deverá estar previsto na configuração do appliance/servidor que será implementado pela CONTRATANTE no ambiente da CONTRATADA;
- 5.4.1.6 Não haverá limitação de quantitativo de servidores e computadores a serem protegidos, a limitação se dará conforme volume de dados da franquia;
- 5.4.1.7 A CÓPIA do backup entre o ambiente do CONTRATANTE e o Data Center da CONTRATADA deverá ocorrer através de um link de dados (intranet ou internet) de no mínimo 30Mbps com 100% de download e upload garantido, dedicado exclusivamente para este fim, sendo de responsabilidade da CONTRATADA a instalação e o custeio do mesmo durante todo o período de contrato;
- 5.4.1.8 Realizar a análise do ambiente atual da CONTRATANTE (identificando modo de operação) e efetuar ajustes no ambiente de backup caso necessário;
- 5.4.1.9 Prestar todo o suporte técnico necessário para a perfeita execução do backup e/ou sua restauração e configuração;
- 5.4.1.10 Realizar a recuperação (restauração) dos dados (da base de dados completa ou apenas arquivos específicos) sempre que demandado pela CONTRATANTE e sem custos adicionais;
- 5.4.1.11 Trafegar os dados do backup sempre de forma segura, utilizando padrões de criptografia;
- 5.4.1.12 Ao final do contrato, todos os dados deverão ser apagados do servidor de Backup, sem possibilidade de recuperação, utilizando DELEÇÃO por "ZERO FILL" garantindo a integridade SIGLOSA do serviço;

5.4.1.13 Deverá ser utilizado software de backup profissional, atendendo todos os requisitos especificados no item “Proteção e Recursos”;

**5.4.2 Proteção e Recursos**

- 5.4.2.1 A solução deve possuir agente remoto para servidores Windows e Linux, suportando as seguintes versões:
  - 5.4.2.1.1 Windows 8.1, Windows 10, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019;
  - 5.4.2.1.2 Red Hat Enterprise Linux (RHEL) 6.3 e superior, CentOS 6.3 e superior, Oracle Linux 6.3 e superior, Debian Linux 7 e superior, Ubuntu 12.04 e superior, SuSE Linux Enterprise Server 11 SP2 e superior, nas plataformas de 32 e 64 bits;
- 5.4.2.2 O software deve possuir agente remoto para Microsoft Exchange, devendo:
  - 5.4.2.2.1 Suportar Exchange 2007 SP1 Rollup 5 e superior;
  - 5.4.2.2.2 Restaurar caixas postais individuais e mensagens específicas de correio eletrônico sem a necessidade de se restaurar toda a base de correio do Exchange (restore granular);
  - 5.4.2.2.3 Permitir redirecionar a restauração para um outro servidor Exchange;
- 5.4.2.3 O software deve possuir agente remoto para Microsoft Sharepoint, devendo:
  - 5.4.2.3.1 Suportar as versões 2007 e superior;
  - 5.4.2.3.2 Suportar Sharepoint Server e Sharepoint Services;
  - 5.4.2.3.3 Através da interface gráfica, restaurar documentos individuais, sites, sub-sites, listas, itens de listas e calendários, sem a necessidade de se restaurar toda aplicação;
- 5.4.2.4 O software deve possuir agente remoto para banco de dados Microsoft SQL, devendo:
  - 5.4.2.4.1 Suportar as versões 2008 e superiores;
  - 5.4.2.4.2 Suportar a funcionalidade de banco de dados em cluster usando Microsoft Cluster Server;
- 5.4.2.5 O software deve possuir agente remoto para Oracle Database, devendo suportar a versão do Oracle12c no sistema operacional Windows 2012 R2 e superior;
- 5.4.2.6 Permitir a execução de backup de arquivos abertos em Windows, mesmo que estejam sendo alterados durante a operação de backup, sem necessidade de suspender a utilização das aplicações pelos usuários nem a conexão da rede. A cópia do arquivo salvo deverá ser idêntica ao arquivo residente em disco, quando do início da operação de backup;
- 5.4.2.7 O software deve ter a capacidade de realizar a verificação da consistência dos backups realizados das aplicações Microsoft Exchange, Microsoft SQL, e em qualquer outro bloco de dados “backupeado”, no intuito de garantir a integridade dos dados;
- 5.4.2.8 Caso seja encontrada uma falha no teste de consistência, o software deverá notificar o administrador para que seja verificado o problema ocorrido nos registros (logs) da ferramenta;
- 5.4.2.9 O snapshot do backup deve ter uma flag identificando a não consistência do backup;
- 5.4.2.10 O Software de backup deve possuir capacidade de replicação nativa que envia backups compactados, de duplicados e, opcionalmente criptografados para um ou vários servidores de backup de destino;
- 5.4.2.11 Em caso de falha de um servidor de backup os agentes devem possuir a capacidade de direcionar os dados para outro servidor que compõe a estrutura de replicação de dados;
- 5.4.2.12 Caso a replicação para outro servidor de backup exigir licenciamento adicional, a solução deverá ser ofertada com licenciamento para que seja possível fazer a replicação para no mínimo 5 (cinco) servidores de backup;
- 5.4.2.13 Possuir tecnologia de desduplicação nativa da solução, devendo desduplicar os dados de forma global;
- 5.4.2.14 A desduplicação deve ser compatível também com backup das aplicações Microsoft Exchange, Microsoft Sharepoint e máquinas virtuais VMWare e Hyper-V;
- 5.4.2.15 Possuir compressão nativa da solução de backup, de forma a minimizar o tamanho dos backups realizados;
- 5.4.2.16 Possuir módulo nativo de criptografia dos dados protegidos, de forma a protegê-los de acesso e uso não autorizado;

- 5.4.2.17 O número de chaves de criptografias que podem ser criadas e armazenadas no sistema para fazer a proteção dos dados deve ser ilimitado e deve possibilitar que a criptografia dos dados seja realizada usando o algoritmo AES de 256 bits;
- 5.4.2.18 A solução deve possuir assistentes de configurações para auxiliar o administrador a automatizar no mínimo as seguintes tarefas:
- 5.4.2.18.1 Assistente de início rápido: auxiliar a configuração para proteger as máquinas, para configurar a replicação de novos agentes, para exportar dados protegidos para máquinas virtuais, para criptografar os dados de ponto de recuperação, para configurar grupos de notificação de e-mail e para configurar uma política de retenção;
  - 5.4.2.18.2 Assistente de proteção de máquinas: orienta o usuário a realizar a proteção de uma ou mais máquinas;
  - 5.4.2.18.3 Assistente de replicação, orientando o usuário a realizar a configuração da replicação de um "Core" primário de modo que uma cópia dos dados protegidos esteja sempre disponível em um outro "Core" separado;
  - 5.4.2.18.4 Assistente de restauração, orientando o usuário durante o processo de restauração de dados a partir de um ponto de recuperação do Core para uma máquina protegida, ou iniciar uma restauração bare metal;
  - 5.4.2.18.5 Assistente e exportação, orientando o usuário a realizar a exportação de um ponto de restauração de uma máquina protegida para qualquer formato VM suportado;
- 5.4.2.19 Deverá permitir, em nível de software, o envio automático de alertas, quando da falha de um procedimento de backup ou restore, através de mensagens de correio eletrônico;
- 5.4.2.20 Possuir recurso do próprio fabricante para download e instalação de updates, upgrades e novas versões do produto, de forma manual ou automática;
- 5.4.2.21 Capacidade de efetuar backups para disco, através de políticas pré-definidas e agendadas;
- 5.4.2.22 Os discos poderão ser discos locais dos servidores, ou discos compartilhados através de infraestruturas do tipo SAN (Storage Area Network), DAS (Direct Attached Storage), NAS (Network Attached Storage) e sistemas de disco compartilhados em infraestruturas externas (baseados em cloud storage ou nuvem);
- 5.4.2.23 O software de backup deve realizar a proteção dos dados no conceito de snapshots podendo configurar o intervalo de tempo entre a geração dos mesmos, sendo o intervalo mais agressivo de no mínimo 10 minutos;
- 5.4.2.24 Em caso de restauração a ferramenta de backup deve fornecer a funcionalidade de restauração online com a possibilidade de utilização imediata do arquivo mesmo que os blocos não estejam totalmente restaurados;
- 5.4.2.25 Possuir suporte aos protocolos de rede IPv4 e IPv6 para rotinas de backup e restore;
- 5.4.2.26 Possuir funcionalidade de arquivamento (archiving) para dispositivos de storage e/ou nuvem, possuindo suporte aos provedores de nuvem Azure, Amazon S3, Rackspace e Openstack;
- 5.4.2.27 Possibilitar o gerenciamento das tarefas de snapshots com recursos de Pause, Hold com data de reativação programada, Stop e Start;
- 5.4.2.28 A solução de backup deve suportar as ferramentas de virtualização VMware vSphere ESXi 5.5 e superior, VMware Workstation 7 e superior, Oracle Virtual Box 5.1 e superior, e Microsoft Hyper-V 2012 R2 e superior;
- 5.4.2.29 A solução de backup deve ser capaz de criar e manter uma máquina virtual em espera (standby), com uma cópia clone do último snapshot do servidor em produção;
- 5.4.2.30 As tarefas de backup e restauração do VMWare deverão ser realizadas via interface gráfica e sem necessidade de scripts.
- 5.4.2.31 Possuir módulo de recuperação de desastres nativo do produto que em caso de falha no equipamento, poderá restaurar o sistema, drivers e dados mesmo em hardware diferente ou máquina virtual;
- 5.4.2.32 Possuir módulo de conversão de backups para máquina virtual (B2V) ou conversão direta para máquina virtual (P2V) nativo da solução de backup;
- 5.4.2.33 O software de backup deve gerar e armazenar logs (registros) das atividades de backup realizadas, visualizados através de uma interface web, podendo exportar os logs;

