



DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

**ANEXO I**  
**TERMO DE REFERÊNCIA**

**Solução Integrada de Tecnologia da Informação para Modernização do TCMPA**

---

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Sumário

1. <u>OBJETO</u> .....	<u>19</u>
2. <u>JUSTIFICATIVA</u> .....	<u>19</u>
0 DA CLASSIFICAÇÃO DOS BENS E SERVIÇOS E DA NATUREZA DA CONTRATAÇÃO	
22	
4. ALINHAMENTO ESTRATÉGICO INSTITUCIONAL.....	22
5. DO RECURSO PARA A DESPESA.....	22
6. <u>DO PARCELAMENTO DO OBJETO</u> .....	<u>23</u>
7. <u>DAS ESPECIFICAÇÕES DO OBJETO</u> .....	<u>24</u>
8. <u>ESPECIFICAÇÕES TÉCNICAS</u> .....	<u>28</u>
8.1. <u>NORMAS TÉCNICAS A SEREM SEGUIDAS NA EXECUÇÃO DOS SERVIÇOS</u> .....	<u>28</u>
8.2. <u>RACK INTELIGENTE</u> .....	<u>30</u>
<u>8.3. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE RACK INTELIGENTE</u> .....	<u>43</u>
8.4. <u>SISTEMA UPS MODULAR DE 150 KVA/150KW</u> .....	<u>47</u>
<u>8.5. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SISTEMA UPS MODULAR DE 150 KVA/150KW</u> .....	<u>49</u>
<u>8.6. PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL</u> .....	<u>50</u>
8.7. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DO ITEM DE PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL.....	79
<u>8.8. SERVIDOR DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS DEFINIDO POR SOFTWARE</u> .....	<u>81</u>
8.8.1.1. Permitir escalabilidade horizontal, isso é, a adição de novos chassis e novos servidores (nós) ao cluster através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao hipervisor, além de crescer de forma linear o desempenho/performance do ambiente;.....	81
8.8.1.2. O procedimento para expansão do cluster deverá ocorrer na mesma interface com assistente que permita tratar as configurações de endereços de rede e garanta que as versões já empregadas no cluster existente sejam transferidas para os novos equipamentos.....	81
8.8.1.3. Permitir adição de um nó por vez.....	81
8.8.1.4. Permitir adição de nós que incrementem apenas o armazenamento do cluster de forma independente do processamento e memória.....	81
8.8.1.5. Permitir adição de novos equipamentos com geração mais recente no mesmo cluster.....	81
8.8.1.6. Permitir remover equipamento do cluster sem parada no ambiente.....	81
8.8.1.7. Criar um cluster lógico, agregando todos os discos físicos dos servidores contidos neste conjunto, apresentando um único sistema de arquivos ao hipervisor.....	81

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.8.1.8.	O item ofertado deve possuir funcionalidade para expor camada de armazenamento para aplicações físicas (bare metal) através do protocolo iSCSI ou NFS ou SMB.....	81
8.8.1.9.	Deverá suportar pelo menos dois Hipervisores. O item ofertado deve oferecer capacidade de conversão de clusters e de cargas de trabalho de um hipervisor para outro a fim de permitir adequação de custos durante renovações de suporte das licenças fornecidas ou aquisição de novas tecnologias de virtualização, preservando o investimento realizado.....	82
8.8.1.10.	Deverão ser fornecidas licenças necessárias para utilização de técnicas de otimização de armazenamento, como por exemplo, compressão e deduplicação.....	82
8.8.1.11.	Deverá garantir replicação síncrona de todos os dados gravados localmente para outros servidores que compõem o cluster para redundância dos dados, cada qual com seu respectivo sistema de armazenamento local com garantia de que a promoção e a demção dos dados ocorram simultaneamente nos servidores do cluster.....	82
8.8.1.12.	A falha ou remoção de um disco não deve interromper o funcionamento de outros discos no mesmo equipamento. Caso o item proposto não atenda este requisito, deverá ser dimensionado prevendo tolerância a falha simultânea de dois equipamentos no mesmo cluster.....	82
8.8.1.13.	Todos os nós do cluster devem participar das operações de reconstrução de disco (rebuild), deixando-os mais eficientes à medida que o cluster cresce em número de nós. Caso o item proposto não atenda a este requisito, deverá ser ofertado com discos de até 3TB (três terabytes) a fim de minimizar o impacto e o tempo de reconstrução.....	82
8.8.2.1.	Permitir operações de live migration (migração da máquina virtual para outro host com a máquina virtual em operação);.....	82
8.8.2.2.	Disponibilizar gerenciador de imagens através de um repositório centralizado e permitir o uso de discos ou imagens nos formatos qcow, qcow2, vmdk, VHD, VHDx, raw, ISO para que seja possível a utilização destes discos e imagens com as máquinas virtuais do cluster;.....	82
8.8.2.3.	O item proposto deve ser capaz de distribuir os servidores virtuais entre os nós do cluster de modo que ocorra distribuição da carga.....	82
8.8.3.1.	Posicionamento inicial: a melhor posição em um cluster para inicialização da máquina virtual ou carga de trabalho;.....	83
8.8.3.2.	Otimização de tempo de execução: movimento de cargas de trabalho com base em métricas durante tempo de execução.....	83
8.8.4.1.	Computação (CPU/MEM).....	83
8.8.4.2.	Utilização da CPU.....	83
8.8.4.3.	Utilização de memória.....	83
8.8.4.4.	Contenção de recursos.....	83
8.8.4.5.	Limiares e/ou marcas d'água para métricas de computação.....	83
8.8.4.6.	Desempenho de armazenamento.....	83
8.8.4.7.	Utilização do processo de gestão das operações de I/O.....	83
8.8.4.8.	Propriedade do disco virtual.....	83
8.8.4.9.	Localização dos volumes.....	83

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.8.4.10.	Regras de afinidade e anti-afinidade .....	83
8.8.4.11.	Políticas definidas pelo usuário para o local (host) onde será executada a VM .....	83
8.8.4.12.	Agrupamento de VMs .....	83
8.8.4.13.	Separação de VMs .....	83
8.8.7.1.	Número de pacotes unicast transmitidos e recebidos; .....	83
8.8.7.2.	Número de pacotes transmitidos e recebidos com um erro; .....	83
8.8.7.3.	Número de pacotes transmitidos e recebidos que foram descartados; .....	83
8.8.31.1.	Compartilhamento através de protocolos NFSv3 e NFSv4 e SMBv2 e SMBv3. Deverá estar devidamente dimensionada para suportar o número de 1.500 (um mil e quinhentos) usuários conectados de forma simultânea; .....	86
8.8.64.1.	Tendência de capacidade, com foco no que foi consumido e como foi na linha do tempo; .....	88
8.8.64.2.	Idade dos arquivos, demonstrando cálculo de quando o arquivo foi alterado pela última vez e a porcentagem dos dados baseado no intervalo de variação de sua idade; .....	88
8.8.64.3.	Detecção de anomalias, demonstrando todas as operações que excedem uma determinada política pré-determinada, como a deleção de múltiplos arquivos em um intervalo menor do que 1 (uma) hora; .....	88
8.8.64.4.	Distribuição por tamanho e tipo de arquivo; .....	88
8.8.64.5.	Ranking dos usuários mais ativos no sistema de armazenamento; .....	88
8.8.64.6.	Ranking dos arquivos mais acessados no sistema de armazenamento; .....	88
8.8.64.7.	Lista das operações mais frequentes (criação, escrita, leitura, deleção e alteração de permissionamento) seja pela média, tendência ou pico da operação;" .....	89
<b><u>8.9.SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SERVIDOR DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS DEFINIDO POR SOFTWARE .....</u></b>		<b>94</b>
8.10.	<b><u>SWITCH CORE CHASSIS MODULAR .....</u></b>	<b>95</b>
8.11.	<b><u>SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 1 .....</u></b>	<b>99</b>
8.12.	<b><u>SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 2 .....</u></b>	<b>100</b>
8.13.	<b><u>SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 3 .....</u></b>	<b>100</b>
8.14.	<b><u>SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 4 .....</u></b>	<b>100</b>
8.15.	<b><u>SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH CORE .....</u></b>	<b>100</b>
8.16.	<b><u>SWITCH DE AGREGAÇÃO .....</u></b>	<b>101</b>
8.17.	<b><u>SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH DE AGREGAÇÃO .....</u></b>	<b>106</b>
8.18.	<b><u>SWITCH DE ACESSO - TIPO 1 .....</u></b>	<b>107</b>
8.19.	<b><u>SWITCH DE ACESSO - TIPO 2 .....</u></b>	<b>111</b>

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

<u>8.20. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH DE ACESSO TIPO 1 ou TIPO 2.....</u>	<u>116</u>
8.21. <u>TRANSCEIVER - TIPO 1.....</u>	<u>117</u>
8.22. <u>TRANSCEIVER - TIPO 2.....</u>	<u>118</u>
8.23. <u>TRANSCEIVER - TIPO 3.....</u>	<u>118</u>
8.24. <u>TRANSCEIVER - TIPO 4.....</u>	<u>119</u>
8.25. <u>TRANSCEIVER - TIPO 5.....</u>	<u>119</u>
8.26. <u>TRANSCEIVER - TIPO 6.....</u>	<u>120</u>
8.27. <u>TRANSCEIVER - TIPO 7.....</u>	<u>120</u>
8.28. <u>TRANSCEIVER - TIPO 8.....</u>	<u>120</u>
8.29. <u>TRANSCEIVER - TIPO 9.....</u>	<u>121</u>
8.30. <u>CABO PARA CONEXÃO DIRETA – TIPO 1.....</u>	<u>121</u>
8.31. <u>CABO PARA CONEXÃO DIRETA – TIPO 2.....</u>	<u>122</u>
8.32. <u>CABO PARA CONEXÃO DIRETA – TIPO 3.....</u>	<u>122</u>
8.33. <u>PONTO DE ACESSO SEM FIO - TIPO 1.....</u>	<u>122</u>
<u>8.34. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE PONTO DE ACESSO SEM FIO TIPO 1.....</u>	<u>127</u>
8.35. <u>PONTO DE ACESSO SEM FIO - TIPO 2.....</u>	<u>128</u>
<u>8.36. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE PONTO DE ACESSO SEM FIO TIPO 2.....</u>	<u>132</u>
<u>8.37. GERENCIAMENTO UNIFICADO DE INFRAESTRUTURA DE REDE LAN E WLAN, CONTROLE DE ACESSO DE USUÁRIOS WIRELESS, ORQUESTRAÇÃO E APROVISIONAMENTO AUTOMÁTICO.....</u>	<u>133</u>
<u>8.38. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE GERENCIAMENTO UNIFICADO DE INFRAESTRUTURA DE REDE LAN E WLAN, CONTROLE DE ACESSO DE USUÁRIOS WIRELESS, ORQUESTRAÇÃO E APROVISIONAMENTO AUTOMÁTICO.....</u>	<u>142</u>
8.39. <u>CÂMERA IP - TIPO 1.....</u>	<u>142</u>
8.40. <u>CÂMERA IP - TIPO 2.....</u>	<u>144</u>
8.41. <u>CÂMERA IP - TIPO 3.....</u>	<u>146</u>
8.42. <u>CÂMERA IP - TIPO 4.....</u>	<u>148</u>
8.43. <u>SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE CÂMERA IP - TIPO 1, 2, 3 ou 4.....</u>	<u>151</u>
8.44. <u>CÂMERA IP - TIPO 5.....</u>	<u>152</u>
8.45. <u>CÂMERA IP - TIPO 6.....</u>	<u>155</u>
8.46. <u>CÂMERA IP - TIPO 7.....</u>	<u>158</u>

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.47. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE CÂMERA IP - TIPO 5, 6 ou 7.....	163
8.48. <u>SOLUÇÃO DE GERENCIAMENTO DE VIDEOMONITORAMENTO VMS</u> .....	<u>163</u>
8.48.1. A Solução de gerenciamento de videomonitoramento VMS deve conter no mínimo as seguintes características:.....	163
8.48.2. Solução de sistema de vídeo segurança deve ser integrado, multiusuário e multi-site. Deve suportar um número ilimitado de servidor de gravação e visualização de câmeras IP, codificadores de vídeo IP; 163	
8.48.3. Gerenciamento otimizado de armazenamento de vídeo: A solução deve dispor de arquivamento único, gravação de longa duração de bom desempenho, escalabilidade e custo-eficiente; 163	
8.48.4. Detecção automática de modelo de câmera: Deve suportar mais de 10000 modelos de câmeras IP, codificadores de vídeo IP, e mais de 150 fornecedores diferentes, utilizando métodos como a Universal Plug and Play, Broadcast, varredura manual e varredura por faixa de IP; .....	163
8.48.5. Número ilimitado de servidores de gravação: Deve suporta um número ilimitados de câmeras por servidor. Gravação continua ou ativada por movimento, evento ou agendamento; .....	164
8.48.6. Rede e armazenamento otimizados: Deve suportar multi-streaming que otimiza a banda usando novos métodos de compressão; MPEG4, H.264, H.265 além MJPEG e MPEG4; .....	164
8.48.7. Deve suportar a utilização de múltiplos fluxos de vídeo de cada câmera para ao visualização e gravação com diferentes configurações de modo a otimizar largura de banda e armazenamento; ..	164
8.48.8. Deve ser capaz de armazenar conteúdo em vídeo que não são críticos em diferentes topologias e arquitetura de armazenamento;.....	164
8.48.9. Deve suportar a detecção de movimento, independente do modelo da câmera; seja pelo servidor ou pela camera; ou simultaneamente;.....	164
8.48.10. Deve ter capacidade de trabalhar com múltiplos sites independentes através da federação dos mesmos em um único site central, garantindo o monitoramento e gestão dos dispositivos de forma unificada. A plataforma/Licença que interconecta sistemas remotos/menores ao site central permitindo um número ilimitado de dispositivos conectados a um sistema central.....	164
8.48.11. Deve suportar comunicação criptografada entre todos os elementos do sistema com chaves geradas por entidades certificadas externas.....	164
8.48.12. Plataforma Aberta: Deve fornecer API / SDK de forma gratuita e suportar integração com hardware ou aplicativos de terceiros.....	164
8.48.13. Integração nativa de todos os dispositivos compatíveis com os fóruns de compatibilidade Onvif Profile S, Q e T e PSIA.....	164
8.48.14. Instalação em Windows 64 bits.....	164
8.48.15. Compatível com Instalações em ambiente virtualizado VMWare e Microsoft Hyper-V	164
8.48.16. Deve permitir exibição do alerta gerado pelos dispositivos, através do processamento dos metadados recebido das câmeras / encoders, mostrando os quadros (overlay) nos formatos e cores gerados pelos dispositivos. Tudo isto deve ser permitido através do dispositivo integrado via ONVIF.	

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.48.17. Deve permitir a integração de sistemas de controle de acesso de forma bi-direcional sem a necessidade de interfaces físicas para tal. Deve permitir que alarmes do sistema de acesso sejam visto na interface do usuário do Sistema de Vídeo assim como o vídeo e os alarmes do mesmo sejam vistos na interface do Sistema de Acesso. ....	164
8.48.18. Permitir integração com Solução de Vídeo Wall com número ilimitado de monitores; .	164
8.48.19. Deve possibilitar total compatibilidade com, no mínimo, duas versões anteriores do sistema;	164
8.48.20. O sistema deve conter os componentes a seguir .....	164
8.48.21. Serviço de Administração .....	164
8.48.22. Gerenciamento centralizado: O software de administração deve oferece um acesso único e consolidado para configuração dos servidores de gravação, mesmo em instalações multisites; .....	165
8.48.23. Assistentes de configuração: Guia o usuário através do processo de adição de câmeras, a configuração de vídeo e gravação, ajuste de detecção de movimento e configuração do usuário; .....	165
8.48.24. Detecção automática de dispositivos: permite a detecção rápida de dispositivos e câmeras usando métodos como a Universal Plug and Play, Broadcast e varredura por faixa de IP; .....	165
8.48.25. Opção de configuração em massa: Altera as configurações em vários dispositivos ao mesmo tempo com poucos cliques; independentemente de estarem no mesmo site ou em sites remotos;	165
8.48.26. Gerenciamento de senhas dos dispositivos diretamente na interface do software. O sistema deve permitir automação de troca periódica das senhas dos dispositivos. ....	165
8.48.27. Importação de dados de configuração off-line: Permite a edição off-line de dados de configuração, incluindo câmeras e as definições de dispositivos; .....	165
8.48.28. Sistema automático de pontos de restauração: um ponto de restauração é criado a cada vez que uma mudança de configuração é feita. Permite a reversão fácil de pontos de configuração previamente definidos e permite o cancelamento de mudanças de configuração indesejados e a restauração de configurações anteriores válidas;.....	165
8.48.29. Deve permitir a personalização da interface de administração de acordo com os direitos de cada usuário, concedendo permissões, restringindo funções e ocultando / desabilitando partes da interface para evitar o acesso indevido a ações restritas. ....	165
8.48.30. Deve permitir a atualização de firmware de câmeras diretamente da interface do VMS . Deve permitir atualização por câmera individualmente ou por grupo de câmeras do mesmo fabricante.	165
8.48.31. Ser nativamente compatível com Microsoft Active Directory para gestão de usuários e perfis de acesso do Windows e permitir autenticação de usuário única (SSO) .....	165
8.48.32. Permitir controle de acesso aos perfis de usuários: Visualização ao vivo, controle PTZ, presets PTZ, controle de saídas, Eventos, ouça o microfone, fale com a caixa de som remota, gravação manual; Reprodução, exportação AVI, exportação JPG, exportação de banco de dados, sequências, pesquisa inteligente e áudio. Bem como definir as vistas, editar vistas particulares e públicas. ....	165
8.48.33. Trabalhar com banco de dados centralizado de fabricantes reconhecidos de mercado como SQL Server, Oracle ou MySQL .....	165

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.48.34.	Deve permitir acesso remoto para o software de visualização e aplicativo para visualização em web browsers, com opção de conexão segura no acesso à câmera (HTTPS).....	165
8.48.35.	Ter servidor de Web embutido para download de softwares e plug-ins.....	165
8.48.36.	Ter histórico de provas exportadas por usuário e arquivo.....	165
8.48.37.	Ter histórico de atividade do usuário do cliente pelo tempo, localidade e câmeras.....	165
8.48.38.	Pode ser instalado em conjunto com o servidor de gravação.....	165
8.48.39.	Fornecer streams múltiplos de vídeo ao vivo para diferentes clientes.....	166
8.48.40.	Serviço de Servidor Móvel.....	166
8.48.41.	O sistema deve suportar.....	166
8.48.42.	Acesso remoto para clientes móveis.....	166
8.48.43.	Realiza o login e solicitações de acesso entre clientes e o Servidor Master.....	166
8.48.44.	Redimensiona as imagens de vídeo vigilância para ajustar ao layout da tela dos dispositivos móveis.....	166
8.48.45.	Pode ser instalado em conjunto do servidor de gravação.....	166
8.48.46.	Deve permitir ser instalado em dispositivos com sistema operacional iOS, Android e Windows Phone.....	166
8.48.47.	Deve permitir a transmissão de imagens geradas em tempo real pela câmera do dispositivo móvel para a central de monitoramento, e gravar estas imagens no sistema como se fosse um dispositivo fixo já instalado no sistema.....	166
8.48.48.	Deve permitir a Inclusão do geo posicionamento através de meta dados de GPS advindos do dispositivo móvel.....	166
8.48.49.	Deve permitir eventos/alarmes no dispositivo móvel em tempo real;.....	166
8.48.50.	Serviço de Gestão de Eventos e Alarmes.....	166
8.48.51.	Deve ter um motor (engine) que forneça regras para a automação de diferentes aspectos do sistema, incluindo controle da câmera, comportamento do sistema e dispositivos externos, com base em eventos ou horários.....	166
8.48.52.	Deve fornecer uma caixa de diálogo de configuração no estilo Microsoft Outlook, na qual eventos predefinidos e personalizados são usados nas regras para acionar ações.....	166
8.48.53.	Teve ter as seguintes categorias de eventos:.....	166
8.48.54.	Ter gerenciamento de evento / alarme de ponto único: gerenciamento central de todos os alarmes internos do sistema e alarmes externos de segurança.....	166
8.48.55.	Ter suporte à associação de alarmes a mapas.....	166
8.48.56.	Deve possuir um Gerenciador de Alarmes que permita.....	166
8.48.56.1.	Relatórios de tratamento de alarmes, fornecendo informações sobre a entrada e o desempenho do tratamento de alarmes.....	167
8.48.57.	Serviço de Gravação e gerenciamento das gravações.....	167
8.48.58.	O sistema deve suportar.....	167

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.48.59.	Gravação digital simultânea de vários canais de vídeo e áudio.....	167
8.48.60.	Transmissão de áudio bidirecional do microfone do cliente para alto-falantes remotos.	167
8.48.61.	A otimização da largura de banda devido ao multi-streaming, dividindo o fluxo de vídeo da câmera para fluxos diferenciados para ver vídeo ao vivo e gravado.....	167
8.48.62.	O software client pode solicitar a visualização ao vivo em uma taxa de quadros diferentes e em resolução mais baixa que as configurações de gravação.....	167
8.48.63.	Conectividade para as câmeras, codificadores de vídeo e DVRs suportando compressões como MJPEG, MPEG4, MPEG4 ASP, H.264 e MxPEG, H.265.....	167
8.48.64.	Detecta automaticamente os modelos de câmeras durante a instalação.....	167
8.48.65.	Número ilimitado de câmeras instaladas.....	167
8.48.66.	Tecnologia de gravação: banco de dados seguro de alta velocidade de imagens JPEG ou fluxos MPEG4 e H264 incluindo áudio.....	167
8.48.67.	Velocidade de gravação: Mais de 30 frames por segundo por câmera, limitado apenas pelo hardware e rede.....	167
8.48.68.	A qualidade da gravação depende inteiramente da câmera e do encoder: não há limitação de software.	167
8.48.69.	Capacidade de gravação ilimitada, dependendo apenas da capacidade de storage .....	167
8.48.70.	Exportação de vídeo configurável por hora ou diária, com passagem automática opcional para unidade de rede de maior capacidade de armazenamento, com imagens disponíveis para reprodução de forma transparente para o operador .....	167
8.48.71.	Detecção de movimento embutida, em tempo real, com sensibilidade completamente ajustáveis e com zonas de exclusão. Permitindo ativar a gravação com velocidade de frames superior quando é detectado movimento ou quando surge um evento, notificando o alerta por e-mail .....	167
8.48.72.	Gravação manual com início do tempo baseada em critérios pré-definidos e privilégios de acesso.	167
8.48.73.	Pan Tilt Zoom (PTZ) com presets armazenados pelo sistema, sendo em até 50 por câmera.	167
8.48.74.	Ativação de presets e patterns quando acontecem determinados eventos. ....	167
8.48.75.	Programação para ativação do pattern em períodos diferentes: isto é, diferente para dia e noite / semana, etc .....	168
8.48.76.	Varredura PTZ em dispositivos suportados: visualização ou gravação enquanto se move lentamente a partir de uma posição para outra .....	168
8.48.77.	Acione o limpador ou esguicho de água remotamente, nos modelos suportados de PTZ	168
8.48.78.	Em eventos pré-definidos comandos são enviados automaticamente para exibir vídeo ao vivo em computadores remotos. ....	168
8.48.79.	O servidor de gravação é executado como um serviço do Windows. ....	168
8.48.80.	Gravação em multi estágios, permite configurar o sistema para gravar em locais, tempo e taxa de frames diferentes. Permitindo até a redução da taxa de frames automática para atender a demanda de tempo de configuração. ....	168

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.48.81. Recuperação configurável de trechos de vídeo perdidos diretamente da câmera que possui a função de gravação local (seja através de cartão de memória removível ou memória fixa embutida na câmera). 168	
8.48.82. Deve suportar gravação embarcada na câmera (edge storage) em vários fabricantes e em dispositivos ONVIF nos perfis acima mencionados; .....	168
8.48.83. Serviços de conexão remota aos servidores de imagem .....	168
8.48.84. Permitir federação de sistemas independentes do mesmo fabricante, sincronizando a informação de alarmes, usuários, câmeras e gravadores com um sistema central .....	168
8.48.85. Permitir a interconexão de câmeras vindas de sistemas independentes (do mesmo fabricante) para um sistema central, trazendo vídeo ao vivo e gravado e seus alarmes associados. ...	168
8.48.86. Suportar sistemas servidores de gravação de 64 bits, em hardware e software .....	168
8.48.87. Assinatura digital no banco de dados garantindo integridade do vídeo. ....	168
8.48.88. Monitoramento do sistema e do servidor de imagens com relatório das configurações. 168	
8.48.88.1. Redundância da gravação de vídeo. O sistema deve permitir que em caso de falha na gravação dos vídeos, outro assuma, sem a adição de licença para essa função. ....	168
8.48.89. A redundância poderá ser efetuada em um ou vários (N:N) storage exclusivos para essa função, ou pode ser feito nos mesmos gravadores do sistema .....	168
8.48.90. Deve possibilitar mover dispositivos (câmeras ou grupo de câmeras) entre diferentes servidores de gravação; .....	168
8.48.91. Deve mover todos os dispositivos associados; .....	168
8.48.92. Deve dispensar reconfiguração de câmeras. ....	168
8.48.93. Obs.:O serviço de gravação nos servidores de gravação não deve depender da instalação de um banco de dados local para garantir seu funcionamento. ....	168
8.48.94. Software De Visualização De Gravação .....	168
8.48.95. Operação.....	168
8.48.96. O sistema deve suportar .....	168
8.48.97. Visualização ao vivo e reprodução: Clients desde dispositivos móveis a computadores com suporte para visualizar até 100 câmeras de vários servidores ao mesmo tempo. ....	169
8.48.98. Exibições de Janelas/Layouts: Trabalha com exibições contendo até 10x10 câmeras, Hot spot, Matriz, Sequencial, imagens estáticas e ativas, vídeos ao vivo ou gravados, mapas HTML, distribuídos em todos os monitores do computador .....	169
8.48.99. Mapas : Os serviços suportados devem incluir serviços de mapas do Bing, Google e OpenStreetMap. Mapas GIS georreferenciados, como shapefiles, desenhos CAD georreferenciados e construção de mapas com vários níveis de piso, com arquivos tipo dwg e dxf .....	169
8.48.100. Serviço de Mapa OpenStreetMap Off-line: Suporta o uso do servidor OpenStreetMap fornecido pelo proprietário para uso off-line .....	169
8.48.101. PTZ inteligente: controle manual, presets, macros (vá à preset quando evento), patrulhamento com esquemas múltiplos (pattern), comandos para limpador (palheta) e esguicho de água, controle por joystick e teclado/mouse.....	169

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.48.102. Matriz Virtual: exibições de controle de câmara ao vivo em computadores remotos para visualização distribuída .....	169
8.48.103. Controle de Entradas/ Saídas de Alarme: Das câmeras ou dispositivos de I/O, de forma a criar botões/eventos manuais, ou receber sinais de sistemas de intrusão ou controle de acesso. ....	169
8.48.104. Áudio multicanal bidirecional: Ouça áudio ao vivo/gravado com reprodução instantânea no PC cliente e transmita voz pelo microfone a alto-falantes remotos. ....	169
8.48.105. Permite gravação de áudio sincronizada a qualquer canal de vídeo. ....	169
8.48.106. Gravação manual: Baseado em privilégios de acesso definido pelo administrador, os usuários clientes podem manualmente iniciar a gravação de uma câmera por um tempo predefinido.	169
8.48.106.1. Dupla autenticação, exigindo com que o usuário tenha autenticação de um usuário supervisor para conseguir se autenticar no software, protegendo o sistema de acessos indevidos. ....	169
8.48.107. Stream de visualização adaptativo, onde a resolução da câmera é alterada automaticamente quando o operador muda a visualização do modo mosaico para modo único em tela cheia.	169
8.48.108. Capacidade de enviar vídeos ao vivo e gravado para monitores de vídeo wall dentro da própria interface .....	169
8.48.109. Busca, backup e dados seguros .....	169
8.48.110. O sistema deve suportar .....	169
8.48.111. Processamento de gravação: Através da busca de movimento acima do vídeo gravado, PTZ digital com suavização de imagem opcional (apenas no software visualizador).....	169
8.48.112. Backup de Evidência: JPEG, AVI, WAV e formatos de dados nativos com software visualizador stand-alone, criptografia de dados e registros, notas de usuários e impressão de relatórios.	169
8.48.113. Autenticação: contas de usuário do Microsoft Active Directory e nativos.....	170
8.48.114. Autorização: contas de usuário e grupos do Microsoft Active Directory e perfis de usuário nativos (do sistema), todos os privilégios de acesso e controle de ações permitidas no nível da câmera.	170
8.48.115. Histórico: Todas as ações do usuário por tempo, localizações e câmeras, e toda a operação do sistema.	170
8.48.116. Alerta: Notifica os usuários em caso de detecção de movimento ou evento por som, e-mail ou SMS.	170
8.48.117. O sistema deve suportar .....	170
8.48.118. Reprodução de gravações de vídeo e áudio localmente no servidor de gravação. ....	170
8.48.119. Visualização de até 16 câmeras com tempo sincronizado durante a reprodução. ....	170
8.48.120. Pesquisa instantânea em gravações com base na data / hora e atividade .....	170
8.48.121. Pesquisa inteligente unificada, através de detecção de movimento, marcadores(bookmarks), eventos e alarmes. ....	170

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.48.122. Pesquisa Forense por metadados: A pesquisa deve poder utilizar eventos de metadados gerados pelas câmeras como ferramenta de busca de imagens. ....	170
8.48.123. Linha de tempo de atividade com recurso de lupa; possibilitando ampliar ou reduzir a faixa de tempo necessária para dar início a busca por vídeos gravados; .....	170
8.48.124. Pesquisa instantânea em gravações com base na data / hora e atividade / alarme (Video Motion Detection) .....	170
8.48.125. Provas podem ser geradas com relatório impresso, imagem em JPEG, AVI ou no formato proprietário (com visualizador incluso), ou ainda pode exportar vídeo em formato MKV padrão. ....	170
8.48.126. Exportação de gravações de áudio em formato WAV ou AVI .....	170
8.48.127. Exportação de vídeo digital com zoom para visualizar área de interesse, e para minimizar o tamanho do arquivo exportado. ....	170
8.48.128. Criptografia e opção de senha de proteção para as gravações e os arquivos exportados.	170
8.48.128.1. Capacidade de adicionar comentários às provas exportadas, também criptografadas.	170
8.48.129. Possuir interface proprietária, desenvolvida pelo mesmo fabricante e com mesmo código fonte do servidor de gerenciamento e gravação. ....	170
8.48.130. Possuir mesma comunicação/ conceito visual do server side .....	170
8.48.131. Não possuir banco de dados proprietário local no cliente, devendo qualquer informação inerente ao sistema ser armazenada somente no banco de dados do servidor de gerenciamento/ banco de dados SQL Server .....	170
8.48.132. Opção para enviar imagens por e-mail .....	170
8.48.133. Aplicativo de visualização através do Web Browser .....	170
8.48.134. O sistema deve suportar .....	170
8.48.135. Visualização de vídeo ao vivo ou reprodução de gravações para 1 a 16 câmeras simultaneamente, advindos do mesmo ou diferentes servidores. ....	170
8.48.136. Navegação de vídeo avançadas, incluindo reprodução lenta/rápida, salto a data/hora e pesquisa de movimento no vídeo. ....	171
8.48.137. Exibições individuais podem ser definidas pelo usuário em vários layouts: exibição ou reprodução de imagens da câmera de vários servidores simultaneamente na mesma vista .....	171
8.48.138. Vistas compartilhadas podem ser geridas centralmente, através do servidor com permissão de administrador .....	171
8.48.139. Importação de mapas estáticos ou ativos para navegação rápida entre câmeras. ....	171
8.48.140. Controle do relé de saída de alarme .....	171
8.48.141. Visão geral das sequências com movimento detectado e janela de visualização. ....	171
8.48.142. Visão geral de eventos / alertas. ....	171
8.48.143. Controle de câmeras PTZ remotamente, usando também posições pré-determinadas. ....	171
8.48.144. Controle remoto de PTZ por clique em ponto. ....	171
8.48.145. Controle remoto de zoom sinalando um retângulo. ....	171

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.48.146. Assumir controle manual sobre uma câmara PTZ que executa um esquema de patrulhamento; após um período de tempo sem atividade a câmera volta ao seu patrulhamento programado. ....	171
8.48.147. Criar arquivos AVI ou criar imagens JPEG geradas a partir de conteúdo gerado pelo software, seja estas imagens advindas de vídeo ou não; .....	171
8.48.148. Imprimir relatórios de incidentes com os comentários livres e pertinentes ao usuário. ..	171
8.48.148.1. Sistema de login usando nomes de usuário e senhas cadastrados no sistema proprietário ou delegado ao Microsoft Active Directory. ....	171
8.48.149. Matriz de Vídeo .....	171
8.48.150. O sistema deve suportar .....	171
8.48.151. Matriz virtual mostrando o vídeo ao vivo diretamente de no mínimo 04 câmeras por cada tela individual a serem acionadas remotamente por comandos remotos e manuais; .....	171
8.48.152. Seqüência de câmeras tipo FIFO (first-in-first-out) .....	171
8.48.153. Vários eventos podem controlar um monitor de matriz e eventos únicos pode controlar vários monitores. ....	171
8.48.154. Visualizar o vídeo na sua taxa máxima de frames em qualquer codec provido pela câmera. 171	171
8.48.155. Cliente celular .....	171
8.48.156. O sistema deve suportar .....	171
8.48.157. Aplicativos gratuitos para dispositivos baseados em sistema operacional Android (Google), iOS (Apple) e Windows Phone 8 .....	171
8.48.158. Permitir a visualização de múltiplas imagens simultaneamente .....	171
8.48.159. Busca e reprodução de vídeo gravado. ....	171
8.48.160. Toque na tela do dispositivo para zoom digital e diferentes modos de visualização da imagem. 171	171
8.48.161. Controle das funcionalidades PTZ das câmeras. ....	172
8.48.162. Salvar ou compartilhar uma foto do vídeo exibido ao vivo .....	172
8.48.163. Permitir a utilização da câmera de vídeo do dispositivo móvel como um gerador de imagens para o sistema principal .....	172
8.48.164. Opções de Integração .....	172
8.48.165. O sistema deve ser .....	172
8.48.166. Compatível com software de integração de vídeo-vigilância com sistemas ATM ou POS (registro de fluxo de produtos/ pessoas para a gestão de prevenção de perdas e fraudes); .....	172
8.48.167. Compatível com software supervisorio de alarmes e estado de dispositivos para grandes instalações. 172	172
8.48.168. Integrado com sistemas de controle de acesso, alarmes, portões, sistemas de gestão, ótica usando os eventos de I/O, eventos internos, eventos TCP/IP ou por OPC DA .....	172
8.48.169. Ter SDK gratuito para integração do vídeo em outros produtos usando a API para exibir	

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

imagens ao vivo, reprodução de atividades gravadas, mostrar imagens de determinado período de tempo, e buscar por movimento. ....	172
8.48.170. Criar, importação e usar páginas HTML para a navegação entre os pontos de vista ou para ativar a matriz virtual no software de visualização. ....	172
8.48.171. Integrado nativamente com todos os dispositivos listados nos fóruns de compatibilidade Onvif, Profile S e PSIA .....	172
8.48.172. Licenciamento .....	172
8.48.173. Deve estar composto por .....	172
8.48.174. Licença de Sistema .....	172
8.48.175. Obrigatório para a instalação do produto .....	172
8.48.175.1. Deve abranger a instalação de um número ilimitado de servidores usando a mesma licença do software de código e a designação de servidores. ....	172
8.48.176. A licença contempla um número ilimitado de servidores de gravação, softwares clientes, clientes web e aplicativos móveis. ....	172
8.48.177. Não tem validade e ser de propriedade do contratante .....	172
8.48.178. Todos os softwares clientes não deverão ser licenciados e podem ser instalados e utilizados em qualquer número de computadores, de forma gratuita .....	172
8.48.179. Acordo de Manutenção do Produto: Esta licença garante a aquisição e uso de forma gratuita de todas as atualizações dos produtos. Deverá ser adquirida para 3 anos. ....	172
8.48.180. Expansão Do Sistema .....	172
8.48.181. A expansão do sistema não deve ser atrelada a quantidade atual de servidores / câmeras. ....	172
8.48.182. O número de servidores de gravação deve permitir ser ampliado a qualquer momento, sem necessidade de licenciamento adicional, seja local ou remoto. ....	172
8.48.183. O número de câmeras pode ser ampliado independente da quantidade de servidores de gravação e/ou estações de operação do sistema .....	172
8.48.184. O número de clientes de operação e de dispositivos móveis, poderá ser ampliado a qualquer momento sem necessidade de licenciamento adicional .....	173
8.49. <a href="#"><u>LICENÇA GERENCIAMENTO DE VIDEOMONITORAMENTO POR CANAL IP .....</u></a>	<a href="#"><u>173</u></a>
8.49.1. Licença compatível com o software VMS descrito nesta especificação, que atendam todas suas características e funcionalidades; .....	173
8.49.2. Deve ser capaz de ativar 1 (um) canal de câmera IP; .....	173
8.50. <a href="#"><u>LICENÇA GERENCIAMENTO DE VIDEOMONITORAMENTO SUPORTE LPR .....</u></a>	<a href="#"><u>173</u></a>
8.50.1. A licença para gerenciamento de videomonitoramento para LPR deve possuir as seguintes características mínimas: .....	173
8.50.2. Sistema de Leitura de matrícula/placa deve ser do mesmo desenvolvedor da solução de gerenciamento de videomonitoramento VMS descritos nesta especificação técnica para uma melhor integração e funcionamento .....	173

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.50.3.	Deve comparar lista de placas previamente configuradas com as imagens ao vivo capturadas por câmeras de vídeo monitoramento IP homologadas pelo fabricante de software .....	173
8.50.4.	Deve possuir reconhecimento de placas de mais de 100 países e estados em todo mundo. ....	173
8.50.5.	Deve atrelar captura de placa a uma regra de captura e registro de vídeo capturando todo trajeto e captura .....	173
8.50.6.	Criação de listas permitidas, negadas e captura automática de todas placas. ....	173
8.50.7.	Deve apresentar captura ao vivo acompanhado do vídeo também capturado ao vivo .....	173
8.50.8.	Deve possuir módulos de placas para diversos países .....	173
8.50.9.	Deve ser atrelado ao sistema de vídeo monitoramento de software dando capacidade de criação de regras, eventos e alarmes. ....	173
8.50.10.	ODeve possuir funcionalidades de compensação de distorção de vídeo e posição incorreta de placas capturadas de um veículo; .....	173
8.50.11.	Deve ser capaz de armazenar uma sequência de vídeo completa associado ao resultado de reconhecimento de placas;.....	173
8.50.12.	Deve suportar o reconhecimento de placas de todo território nacional; .....	173
8.50.13.	Deve fornecer ajuste de parâmetros de reconhecimento e grau de confiança; .....	173
8.50.14.	Deve ter a capacidade de gerenciamento remoto; .....	173
8.50.15.	Deve suportar listas internas das placas registradas (Branca, Negra e Informativa); .....	173
8.50.16.	Deve fornecer interface flexível ao operador para resolução de diferentes tarefas; .....	173
8.50.17.	Deve fornecer diversos métodos de pesquisa, seja por placa capturada, data e/ou horário e resultados associados com imagens/vídeo das placas; .....	173
8.50.18.	Deve ser capaz de pesquisar por qualquer sequência de caracteres reconhecidos; .....	173
8.50.19.	Deve permitir a busca de múltiplos veículos dentro de uma única busca, dentro de um critério único; .....	174
8.50.20.	Deve ser capaz de pesquisar pela câmera que realizou o reconhecimento de placa; .....	174
8.50.21.	Deve ser capaz de pesquisar por qualquer sequência de caracteres reconhecidos; .....	174
8.50.22.	Deve permitir a configuração de alarmes e/ou eventos baseados no reconhecimento de placas; .....	174
8.50.23.	Deve ter capacidade de integrar com o Sistema de Controle de Acesso obtido através deste edital para permitir o acionamento das cancelas após o reconhecimento da placa veicular; .....	174
8.50.24.	Deve ser compatível com Microsoft® Windows® Server 2016 ou versão mais recente; .....	174

<b>8.51.</b>	<b><u>SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE GERENCIAMENTO DE VIDEOMONITORAMENTO VMS</u></b> .....	<b>174</b>
8.51.1.	Serviço de instalação de software VMS compreende.....	174
8.51.2.	Instalação do software VMS no servidor designado para este fim; .....	174
8.51.3.	Serviço de configurações de software VMS compreendem .....	174

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

8.51.4. Configurações básicas para que o software entre em operação no ambiente proposto, adição das câmeras IP, atribuição de nome, atribuição de IP, configurações de imagens, resolução, qualidade de imagem, streamings de vídeo, configurações de armazenamento, gravação e configurações gerais;	174
8.51.5. Devem ser instaladas e implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades e a configuração do software VMS, explorando suas características, a seguir descritas, dentro das melhores práticas de rede, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação; .....	174
8.52. <u>RACK DE PISO .....</u>	<u>174</u>
8.53. <u>SERVIÇO DE INSTALAÇÃO DE RACK DE PISO .....</u>	<u>175</u>
8.54. <u>RACK DE TETO .....</u>	<u>176</u>
8.55. <u>SERVIÇO DE INSTALAÇÃO DE RACK DE TETO .....</u>	<u>176</u>
8.56. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ELETROCALHA .....</u>	<u>177</u>
8.57. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE SEAL TUBE TIPO I .....</u>	<u>178</u>
8.58. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE SEAL TUBE TIPO II .....</u>	<u>179</u>
8.59. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CANALETA TIPO I .....</u>	<u>179</u>
8.60. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CANALETA TIPO II .....</u>	<u>181</u>
8.61. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA EXTERNA COM ESPELHO TIPO I .....</u>	<u>182</u>
8.62. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA EXTERNA COM ESPELHO TIPO II .....</u>	<u>183</u>
8.63. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ELETRODUTO METÁLICO</u>	<u>184</u>
8.64. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA DE PASSAGEM METÁLICA .....</u>	<u>184</u>
8.65. <u>RACK DE PAREDE 12U .....</u>	<u>185</u>
8.66. <u>SERVIÇO DE INSTALAÇÃO DE RACK DE PAREDE 12U .....</u>	<u>185</u>
8.67. <u>SERVIÇO DE INSTALAÇÃO DE PONTO COM FORNECIMENTO DE CABEAMENTO ESTRUTURADO CATEGORIA 6A .....</u>	<u>186</u>
8.68. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH PANEL MODULAR CATEGORIA 6ª .....</u>	<u>188</u>
8.69. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO I .....</u>	<u>189</u>
8.70. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO II .....</u>	<u>190</u>
8.71. <u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO III .....</u>	<u>191</u>
8.72. <u>SERVIÇO DE CERTIFICAÇÃO DE PONTO LÓGICO .....</u>	<u>192</u>

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO	
8.73.	<u>SERVIÇO DE REORGANIZAÇÃO DE RACKS ATÉ 25 PONTOS.....</u> 194
8.74.	<u>SERVIÇO DE REORGANIZAÇÃO DE RACKS DE 25 ATÉ 50 PONTOS .....</u> 194
8.75.	<u>SERVIÇO DE REORGANIZAÇÃO DE RACKS DE 50 ATÉ 100 PONTOS .....</u> 194
8.76.	<u>SERVIÇO DE IDENTIFICAÇÃO DE PONTO LÓGICO .....</u> 194
8.77.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE "DIO" PARA 12 FIBRAS MM OU SM .....</u> 194
8.78.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE "DIO" PARA 72 FIBRAS MM OU SM .....</u> 195
8.79.	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA DE TERMINACAO OPTICA 196
8.80.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CABO DE FIBRA ÓPTICA INDOOR/OUTDOOR 06FO MM 50/125 OM3 .....</u> 197
8.81.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CABO DE FIBRA ÓPTICA INDOOR/OUTDOOR 12FO MM 50/125 OM3 .....</u> 198
8.82.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE FIBRA ÓPTICA INDOOR/OUTDOOR 06FO SM .....</u> 199
8.83.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE FIBRA ÓPTICA INDOOR/OUTDOOR 12FO SM .....</u> 200
8.84.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD ÓPTICO DUPLEX LC-LC MM 50/125 - OM3 DE 2,5 A 5 MTS .....</u> 201
8.85.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD ÓPTICO DUPLEX LC-LC SM DE 2,5 A 5 MTS .....</u> 202
8.86.	<u>SERVIÇO DE FUSÃO DE FIBRA ÓPTICA .....</u> 203
8.87.	<u>SERVIÇO CERTIFICAÇÃO DE FIBRA ÓPTICA .....</u> 203
8.88.	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PONTOS DE ENERGIA .204
8.89.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE QUADRO DE DISTRIBUIÇÃO ELÉTRICO PARA ATE 28 DISJUNTORES .....</u> 205
8.90.	<u>SERVIÇO DE INTERLIGAÇÃO DE QUADRO ELÉTRICO TRIFÁSICO AO QUADRO GERAL ATÉ 60MTS .....</u> 206
8.91.	<u>SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ATERRAMENTO BÁSICO. 207</u>
8.92.	<u>SERVIÇO DE REMANEJAMENTO DE PONTO LÓGICO OU ELÉTRICO, SEM FORNECIMENTO DE MATERIAIS E INFRA ESTRUTURA .....</u> 207
8.93.	<u>SERVIÇO DE ELABORAÇÃO DE AS-BUILT .....</u> 208
8.94.	<u>TREINAMENTO/REPASSE DE CONHECIMENTO .....</u> 209
9.	<u>HOMOLOGAÇÃO TÉCNICA .....</u> 209
10.	<u>SLA – ACORDO DE NIVEL DE SERVIÇO .....</u> 209
11.	<u>SERVIÇO SUPORTE E ATENDIMENTO .....</u> 210

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

12.	<a href="#">DA VISTORIA</a>	211
13.	<a href="#">DA PARTICIPAÇÃO DE ME E EPP</a>	212
0	DOS CRITÉRIOS DE ELABORAÇÃO DA PROPOSTA COMERCIAL VENCEDORA DOS LANCES	212
15.	<a href="#">DO PRAZO DE ENTREGA / EXECUÇÃO</a>	213
16.	<a href="#">DA ENTREGA E DO RECEBIMENTO DO OBJETO</a>	213
17.	<a href="#">LOCAL DE ENTREGA E EXECUÇÃO DOS OBJETO</a>	214
18.	<a href="#">PRAZO DE VIGÊNCIA E EXECUÇÃO DO CONTRATO</a>	214
19.	MEIOS FORMAIS DE COMUNICAÇÃO	215
20.	SUBCONTRATAÇÃO	215
21.	DO VÍNCULO EMPREGATÍCIO	215
22.	DA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO	216
23.	DAS OBRIGAÇÕES DA CONTRATANTE	216
24.	DAS OBRIGAÇÕES DA CONTRATADA	216
25.	<a href="#">CRITÉRIOS E REQUISITOS DE HABILITAÇÃO</a>	219
25.3.	<a href="#">CONDIÇÕES PARA PAGAMENTO</a>	222
26.	<a href="#">REAJUSTE</a>	223
27.	REEQUILIBRIO ECONÔMICO-FINANCEIRO	224
28.	GARANTIAS	224
29.	DISPOSIÇÕES GERAIS	224

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

## 1. OBJETO

- 1.1. Registro de preços da proposta mais vantajosa para eventual e futura contratação de empresa especializada para implantação de solução que contempla serviços de instalações, fornecimento de materiais, equipamentos e infraestrutura necessárias à solução integrada de tecnologia da informação para modernização do TCMPA incluindo transferência de conhecimento por treinamento da equipe técnica, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência e seus anexos.

## 2. JUSTIFICATIVA

- 2.1. O TCMPA tem atuado na consolidação de sua estrutura organizacional com o intuito de ampliar sua autonomia e promover melhorias na condução de suas atividades operacionais em consonância com as melhores práticas do mercado e da Administração Pública, cujo resultado esperado é maior eficiência na execução de sua missão institucional, que é atuar na fiscalização e controles das contas dos municípios do Estado do Pará, de forma ágil, eficiente e transparente, assegurando a higidez e confiabilidade ao sistema e a atuação do TCMPA. Com fim a atender a missão institucional, o TCMPA criou, internamente, sua própria Diretoria de Tecnologia da Informação, para prover as diretrizes de tecnologia da informação necessárias a todos seus usuários
- 2.2. Os equipamentos são responsáveis por permitir a troca de dados entre os usuários e servidores existentes no ambiente com maior capacidade de processamento/comutação de pacotes e velocidade de links de comunicação, principalmente para permitir a interconexão entre o datacenter do prédio sede e serviços contratados de “cloud”. A interconexão deve ser de alta velocidade.
- 2.3. No âmbito dos Tribunais de Contas, em face da quantidade de jurisdicionados e de dados que são encaminhados para processamento e análise do controle externo, diariamente, a evolução tecnológica se revela ainda mais exigível, a qual vem ocorrendo em uma ascendente exponencial, vocacionada a modernização dos parques de TI e a utilização de ferramentas que exigem ainda mais destes equipamentos, a exemplo do exemplo do *Big Data*, *Business Intelligence* (BI) e *Inteligência Artificial* (IA).
- 2.4. Atualmente há a necessidade de ampliar a quantidade e trazer melhorias nas conexões, aumentar a segurança da rede, aumentar a velocidade das mesmas, atualizar a tecnologia dos equipamentos obsoletos, inclusive por meio de substituição dos quais estão sem a devida manutenção e suporte do fabricante, pois já saíram de linha de produção a mais de 15 (quinze) anos.
- 2.5. A demanda está alinhada com o planejamento da Diretoria de Tecnologia da Informação 2021/2022, inclusive como ferramenta para atingir as metas do TCMPA. Assim, necessária a modernização abrangente e interconexa conforme o presente Termo de Referência, para adequado suporte às atividades desempenhadas.
- 2.6. Sendo assim, faz-se necessário os serviços e as aquisições de TI, conforme as especificações que serão descritas adiante.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 2.7. Com objetivo de atingirmos as metas traçadas, porém mantendo a flexibilidade para adaptações necessárias, que podem ocorrer desde início do processo administrativo e procedimentos após a finalização da disputa do certame, diante ainda de período de pandemia, com surgimento de novas cepas no cenário internacional, e outros fatores podem sobremaneira interferir de forma contundente, os quantitativos foram estimados.
- 2.8. No interregno temporal já mencionado estamos sujeitos a fatores externos com reflexos internos, e necessárias adaptações, por possíveis mudanças de gestão, que podem interferir, se refletindo em alterações quantitativas prováveis. Tal flexibilidade é necessária para atendermos com eficiência, presteza e devida agilidade às necessidades e adaptarmos a eventuais alterações que surgirem como necessárias, e para melhor aproveitamento do processo administrativo de licitação, primando pela sua eficiência, finalidade e economicidade.

**2.9. OBJETIVOS COM A CONTRATAÇÃO**

A contratação pretendida por esta DTI visa a aquisição, implantação, treinamento, integração, contemplando soluções de processamento, armazenamento de dados, solução de segurança de dados perimetral, sistema de videomonitoramento, switches, pontos de acesso sem fio, serviços de cabeamento estruturado e fibra óptica, para ampla e irrestrita modernização da infraestrutura de rede do TCMPA.

Cuida-se, portanto, de uma renovação ampla e sistêmica de toda a planta tecnológica do TCMPA, dado que a esperada contratação se estabelece a partir de uma perspectiva clara de necessidade de consolidação da estrutura organizacional do TCMPA, ampliando sua autonomia, com a clara promoção de melhorias na condução de suas atividades operacionais em consonância com as melhores práticas do mercado e da Administração Pública, cujo resultado esperado é maior eficiência na execução de sua missão institucional, voltada à fiscalização e controles das contas dos municípios do Estado do Pará, de forma ágil, eficiente e transparente, assegurando a higidez e confiabilidade ao sistema e a atuação do TCMPA.

A modelagem adotada junto ao projeto apresentado, leva em consideração as necessidades de modernização da infraestrutura de redes de computadores para todos seus usuários, fornecida por uma camada de conectividade composta por equipamentos comutadores de dados (switches).

Tais equipamentos são responsáveis por permitir a troca de dados entre os usuários e servidores existentes no ambiente com maior capacidade de processamento/comutação de pacotes e velocidade de links de comunicação, principalmente para permitir a interconexão entre o datacenter do prédio sede e serviços contratados de “cloud”, o que de fato não ocorre atualmente, em virtude dos problemas e evidências já pontuados.

Atualmente há a necessidade de ampliar a quantidade de conexões, aumentar a velocidade das mesmas e de ir substituindo equipamentos obsoletos em tecnologia os quais estão sem a devida manutenção e suporte do fabricante, uma vez que já saíram de linha de produção, em média, a mais de 08 (oito) anos, alcançando, em casos críticos, a exemplo do data center, a superação dos 10 (dez) anos de uso.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Compreendemos, portanto, que a presente demanda está alinhada com o planejamento da DTI e, antes disso, da própria gestão para o biênio 2021/2022, a qual somente se dará a partir da modernização, renovação dos equipamentos para suporte às atividades e promoção de melhorias na rede por meio dos *switches*, pontos de acesso sem fio, servidores de processamento e armazenamento de dados, videomonitoramento e segurança de dados, bem como melhoria nos cabeamentos metálicos e ópticos.

Nesta linha, impõem-se a aquisição de novos equipamentos de TI, conforme as especificações constantes do Termo de Referência, preconizando-se os seguintes objetivos troncais:

- 5888** Garantir a integridade física dos ativos de TI que sustentam os sistemas que atendem o TCMPA sob a tutela da DI.
- 5889** Garantir a segurança de TI.
- 5890** Garantir a capacidade de processamento e armazenamento de dados do TCMPA.
- 5891** Garantir a disponibilidade de comunicação na rede de dados do TCMPA.
- 5892** Prover recursos para utilização de novas aplicações e sistemas capazes de tornar mais célere a atuação do Tribunal.
- 5893** Aumentar a velocidade com que as estações de trabalho do Tribunal se comunicam com as aplicações suportadas pela DI.
- 5894** Modernização da rede corporativa;
- 5895** Maior capacidade de transmissão;
- 5896** Maior eficiência dos ativos que compõem a rede corporativa;
- 5897** Padronização dos equipamentos, o que facilitará a administração, documentação e treinamento dos servidores e demais colaboradores terceirizados.

Assim, a contratação agrega a garantia da segurança das informações produzidas e/ou geridas por este órgão bem como a alta disponibilidade aos dados e também a alta capacidade de armazenamento e previsibilidade de eventuais expansões necessária de modo a atender eventuais novidades de aplicações e sistema tornando-se então mais célere a atuação do TCMPA.

Prezando ainda pela padronização dos equipamentos, o que com treinamento dos profissionais responsáveis, trará conhecimento específico da equipe dando maior eficiência na administração, documentação e consequente operação bem como menor tempo de resposta para eventuais manutenções necessária ou recuperação de desastres.

Tornando então a rede corporativa mais eficiente, com maior capacidade de transmissão e comunicação no ecossistema deste Tribunal, preparando-a para as necessidades atuais e de futuro próximo.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

**0 DA CLASSIFICAÇÃO DOS BENS E SERVIÇOS E DA NATUREZA DA CONTRATAÇÃO**

3.1. Os bens e serviços que constituem o objeto deste termo se enquadram no conceito de comuns, nos termos da Lei Federal n.º 10.520/2002, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado.

**4. ALINHAMENTO ESTRATÉGICO INSTITUCIONAL**

4.1. A demanda está alinhada com o Plano Diretor de Tecnologia da Informação 2021/2022.

**4.1.1. RESULTADOS ESPERADOS**

O resultante deste projeto será a melhoria na qualidade dos serviços do sistema de rede de dados ofertados aos clientes internos e externos do TCMPA, atendendo então a necessidade atual da ampliação da rede com a devida atualização tecnológica da solução de processamento, distribuição e segurança da informação, garantindo a disponibilidade e flexibilidade da rede de dados com atendimento a demanda de crescimento dos serviços de Tecnologia da Informação (TI) do TCMPA, que com a atual situação pandêmica ao qual convivemos tem requerido cada vez mais do setor.

Aumento da capacidade de processamento/comutação de pacotes, segurança e velocidade dos links de comunicação, para acesso externo e também para permitir a interconexão entre o datacenter do prédio sede e sua expansão com a máxima eficiência e segurança.

Resultando então em um ambiente seguro, ágil, flexível e disponível ao usuário dentro dos melhores critérios governamentais e atendendo a atual legislação e as melhores práticas de governança da Tecnologia da Informação com um baixo custo operacional e maior parcela de automatização dos processos administrativo do ambiente tecnológico, diminuindo a possibilidade de erros operacionais e consequentes paradas nos serviços.

Resultado este que trará uma melhor experiência ao usuário dando maior produtividade aos colaboradores e consequentemente ao usuário dos serviços prestados pelo TCMPA trazendo maior eficiência nos resultados para toda sociedade Paraense.

**0.0 DO RECURSO PARA A DESPESA**

**0.0.0 339030-MATERIAL DE CONSUMO.**

**0.0.1 339040-SERV.DE TECNO.DA INFOR.E COMUN. -PESS JURIDICA**

**0.0.2 449052-EQUIPAMENTOS E MATERIAL PERMANENTE**

**0 DO PARCELAMENTO DO OBJETO**

6.1. O presente Termo de Referência envolve uma solução: planejamento e execução integrados com equipamentos, softwares, serviços que irão compor uma solução integrada, requerendo para seu pleno funcionamento a total compatibilidade,

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

interoperabilidade, interconectividade, padronização dos produtos e sincronismo de execução das fases de sua implementação.

- 6.2. O fator tecnológico determinante é a interoperabilidade entre os equipamentos, padronização dos serviços, garantias centradas num único fornecedor, com agilidade, e funcionalidade condicionando o agrupamento para atendimento também às condições administrativas de cumprimento de finalidades deste contratante. É ao padrão tecnológico destes equipamentos, materiais e serviços, infraestrutura e acessórios que compõem a solução, sendo de fundamental importância o sucesso da implementação do todo integrado.
- 6.3. A possibilidade de decomposição do objeto em vários processos licitatórios distintos envolveria altíssimo grau de risco de insucesso na implementação da solução, integração e especialmente com relação a riscos na interoperabilidade, dificultando a gestão e eficiência finalística.
- 6.4. Outro aspecto importante é a garantia de compatibilidade e plena integração, que exigiria uma série de restrições e amarrações entre todas as contratações, o que poderia incorrer em perda de competitividade e dificuldades outras a seguir explanadas. O que habitualmente observa-se em casos de contratações desmembradas para este tipo de solução proposta, necessidade de muitas restrições competitivas e, mesmo com todos os cuidados no Edital e termos de referência, a experiência nos tem mostrado, que após a solução instalada ocorre invariavelmente alguma forma de defeito, e os diversos responsáveis passam a se digladiar, com acusações mútuas quanto à responsabilidade pelo vício e sempre alegando que cumpriram o edital e tiveram suas propostas aceitas.
- 6.5. Outro fator importante, que não pode ser deslembrado, é quanto ao sigilo, segurança das informações e intervenções realizadas no órgão, que quanto menor os números de empresas e pessoas envolvidas, menor os riscos, especialmente em tempos de LGPD e necessárias práticas de *compliance* na gestão dos riscos. Cabe ainda frisar que no mercado atuam inúmeras empresas especializadas no mercado de Tecnologia da Informação e as quais propõem soluções integradas, com capacidade para atender a solução na forma proposta neste Termo de Referência sem qualquer prejuízo à competitividade e com ganhos em escala, inclusive.
- 6.6. Outra vantagem ao TCMPA que uma única empresa especializada responsável pelo atendimento da solução integrada com seus respectivos aspectos de implementação e manutenção da estabilidade e operacionalidade de toda a solução, proporciona à Administração ganho em capacidade de gestão do contrato, com melhores instrumentos de cobrança e garantia de efetividade, pois sob a responsabilidade de um único mantenedor de todos os aspectos envolvendo o ambiente instalado. A concentração em um único interlocutor na gestão dos contratos e um único procedimento de chamada de assistência técnica durante o período de garantia, propicia em muito a agilidade na resolução de problemas (com ganhos no aspecto de economicidade) advindos de possíveis e eventuais falhas na solução ou eventos que digam respeito ao contrato.
- 6.7. O atual mercado fornecedor do objeto deste Termo de Referência se encontra perfeitamente enquadrado nessa visão integralizada de serviços com aplicação de materiais ou equipamentos. As empresas se estruturaram como integradoras de soluções

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

e, comumente, representam fabricantes de equipamentos concorrentes por questões de perfis de clientes a serem atendidos, exigindo sempre flexibilidade das empresas especializadas para atenderem às exigências e especificidades de seus clientes, especialmente clientes com grandes demandas e responsabilidades como este TCMPA. Essa situação abriu definitivamente o leque de opções para novas contratações, especialmente no que se refere a projetos de maiores, com certa complexidade técnica, como este, permitindo mais agilidade e melhorias no atingimento das finalidades, o que sem dúvida, acirrará a concorrência no certame, já que muitas empresas poderão oferecer soluções, adequadas às necessidades do TCMPA, proporcionando ganho em escala. Assim, com apenas uma empresa efetivamente CONTRATADA, refuta-se definitivamente a possibilidade de malogro contratual vislumbrada no parágrafo anterior.

**0 DAS ESPECIFICAÇÕES DO OBJETO**

**LOTE ÚNICO**

<b>ITEM</b>	<b>DESCRIÇÃO</b>	<b>UND</b>	<b>QTDE</b>	<b>VAL O R UNIT.</b>	<b>VALOR TOTAL</b>
1	RACK INTELIGENTE	UM	2		
2	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE RACK INTELIGENTE	UM	2		
3	SISTEMA UPS MODULAR DE 150 KVA/150KW	UM	2		
4	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SISTEMA UPS MODULAR DE 150 KVA/150KW	UM	2		
5	SOLUÇÃO DE PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL	UM	2		
6	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SOLUÇÃO DE PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL	UM	2		
7	SERVIDOR DE PROCESSAMENTO E	UM	4		

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

ITEM	DESCRIÇÃO	UND	QTDE	VALOR UNIT.	VALOR TOTAL
	ARMAZENAMENTO DE DADOS DEFINIDO POR SOFTWARE				
8	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SERVIDOR DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS DEFINIDO POR SOFTWARE	UM	4		
9	SWITCH CORE CHASSIS MODULAR	UM	2		
10	SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 1	UM	2		
11	SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 2	UM	2		
12	SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 3	UM	4		
13	SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 4	UM	4		
14	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH CORE	UM	2		
15	SWITCH DE AGREGAÇÃO	UM	2		
16	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH DE AGREGAÇÃO	UM	2		
17	SWITCH DE ACESSO - TIPO 1	UM	40		
18	SWITCH DE ACESSO - TIPO 2	UM	20		
19	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH DE ACESSO TIPO 1 ou TIPO 2	UM	60		
20	TRANSCEIVER - TIPO 1	UM	40		
21	TRANSCEIVER - TIPO 2	UM	20		
22	TRANSCEIVER - TIPO 3	UM	40		
23	TRANSCEIVER - TIPO 4	UM	10		
24	TRANSCEIVER - TIPO 5	UM	10		
25	TRANSCEIVER - TIPO 6	UM	10		
26	TRANSCEIVER - TIPO 7	UM	8		
27	TRANSCEIVER - TIPO 8	UM	8		
28	TRANSCEIVER - TIPO 9	UM	4		
29	CABO PARA CONEXÃO DIRETA – TIPO 1	UM	20		
30	CABO PARA CONEXÃO DIRETA – TIPO 2	UM	20		
31	CABO PARA CONEXÃO DIRETA – TIPO 3	UM	4		
32	PONTO DE ACESSO SEM FIO - TIPO 1	UM	80		
33	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE PONTO DE ACESSO SEM FIO TIPO 1	UM	80		
34	PONTO DE ACESSO SEM FIO - TIPO 2	UM	4		
35	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE PONTO DE ACESSO SEM FIO TIPO 2	UM	4		

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

ITEM	DESCRIÇÃO	UND	QTDE	VALOR UNIT.	VALOR TOTAL
36	GERENCIAMENTO UNIFICADO DE INFRAESTRUTURA DE REDE LAN E WLAN, CONTROLE DE ACESSO DE USUÁRIOS WIRELESS, ORQUESTRAÇÃO E APROVISIONAMENTO AUTOMÁTICO.	UM	1		
37	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE GERENCIAMENTO UNIFICADO DE INFRAESTRUTURA DE REDE LAN E WLAN, CONTROLE DE ACESSO DE USUÁRIOS WIRELESS, ORQUESTRAÇÃO E APROVISIONAMENTO AUTOMÁTICO.	UM	1		
38	CÂMERA IP - TIPO 1	UM	20		
39	CÂMERA IP - TIPO 2	UM	30		
40	CÂMERA IP - TIPO 3	UM	20		
41	CÂMERA IP - TIPO 4	UM	26		
42	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE CÂMERA IP - TIPO 1, 2, 3 ou 4	UM	96		
43	CÂMERA IP - TIPO 5	UM	6		
44	CÂMERA IP - TIPO 6	UM	8		
45	CÂMERA IP - TIPO 7	UM	2		
46	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE CÂMERA IP - TIPO 5, 6 ou 7	UM	16		
47	SOLUÇÃO DE GERENCIAMENTO DE VIDEOMONITORAMENTO VMS	UM	1		
48	LICENÇA GERENCIAMENTO DE VIDEOMONITORAMENTO POR CANAL IP		112		
49	LICENÇA GERENCIAMENTO DE VIDEOMONITORAMENTO SUPORTE LPR		1		
50	SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE VIDEOMONITORAMENTO VMS	UM	1		
51	RACK DE PISO	UM	6		
52	SERVIÇO DE INSTALAÇÃO DE RACK DE PISO	UM	6		
53	RACK DE TETO	UM	14		
54	SERVIÇO DE INSTALAÇÃO DE RACK DE TETO	UM	14		
55	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ELETROCALHA	M	1000		
56	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE SEAL TUBE TIPO I	M	1500		
57	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE SEAL TUBE TIPO II	M	1500		
58	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CANALETA TIPO I	M	750		
59	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CANALETA TIPO II	M	500		
60	SERVIÇO DE INSTALAÇÃO COM	UM	800		

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

ITEM	DESCRIÇÃO	UND	QTDE	VALOR UNIT.	VALOR TOTAL
	FORNECIMENTO DE CAIXA EXTERNA COM ESPELHO TIPO I				
61	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA EXTERNA COM ESPELHO TIPO II	UM	800		
62	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ELETRODUTO METÁLICO	M	500		
63	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA DE PASSAGEM METÁLICA	UM	40		
64	RACK DE PAREDE 12U	UM	2		
65	SERVIÇO DE INSTALAÇÃO DE RACK DE PAREDE 12U	UM	2		
66	SERVIÇO DE INSTALAÇÃO DE PONTO COM FORNECIMENTO DE CABEAMENTO ESTRUTURADO CATEGORIA 6A	PT	960		
67	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH PANEL MODULAR CATEGORIA 6A	UM	60		
68	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO I	UM	400		
69	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO II	UM	400		
70	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO III	UM	300		
71	SERVIÇO DE CERTIFICAÇÃO DE PONTO LÓGICO	UM	960		
72	SERVIÇO DE REORGANIZAÇÃO DE RACKS ATÉ 25 PONTOS.	UM	10		
73	SERVIÇO DE REORGANIZAÇÃO DE RACKS DE 25 ATÉ 50 PONTOS.	UM	10		
74	SERVIÇO DE REORGANIZAÇÃO DE RACKS DE 50 ATÉ 100 PONTOS.	UM	10		
75	SERVIÇO DE IDENTIFICAÇÃO DE PONTO LÓGICO	UM	960		
76	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE "DIO" PARA 12 FIBRAS MM OU SM	UM	4		
77	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE "DIO" PARA 72 FIBRAS MM OU SM	UM	3		
78	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA DE TERMINACAO OPTICA	UM	14		
79	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CABO DE FIBRA ÓPTICA INDOOR/OUTDOOR 06FO MM 50/125 OM3	M	600		
80	SERVIÇO DE INSTALAÇÃO COM	M	600		

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

ITEM	DESCRIÇÃO	UND	QTDE	VALOR UNIT.	VALOR TOTAL
	FORNECIMENTO DE CABO DE FIBRA ÓPTICA INDOOR/OUTDOOR 12FO MM 50/125 OM3				
81	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE FIBRA ÓPTICA INDOOR/OUTDOOR 06FO SM	M	1600		
82	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE FIBRA ÓPTICA INDOOR/OUTDOOR 12FO SM	M	1600		
83	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD ÓPTICO DUPLEX LC-LC MM 50/125 - OM3 DE 2,5 A 5 MTS	UM	12		
84	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD ÓPTICO DUPLEX LC-LC SM DE 2,5 A 5 MTS	UM	64		
85	SERVIÇO DE FUSÃO DE FIBRA ÓPTICA	UM	204		
86	SERVIÇO CERTIFICAÇÃO DE FIBRA ÓPTICA	UM	102		
87	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PONTOS DE ENERGIA	PT	1920		
88	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE QUADRO DE DISTRIBUIÇÃO ELÉTRICO PARA ATE 28 DISJUNTORES	UM	16		
89	SERVIÇO DE INTERLIGAÇÃO DE QUADRO ELÉTRICO TRIFÁSICO AO QUADRO GERAL ATÉ 60MTS	UM	16		
90	SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ATERRAMENTO BÁSICO.	UM	4		
91	SERVIÇO DE REMANEJAMENTO DE PONTO LÓGICO OU ELÉTRICO, SEM FORNECIMENTO DE MATERIAIS E INFRA ESTRUTURA	UM	200		
92	SERVIÇO DE ELABORAÇÃO DE AS-BUILT	UM	2		
93	TREINAMENTO/REPASSE DE CONHECIMENTO	UM	2		
VALOR TOTAL :					

## 8. ESPECIFICAÇÕES TÉCNICAS

### 8.1. NORMAS TÉCNICAS A SEREM SEGUIDAS NA EXECUÇÃO DOS SERVIÇOS

8.1.1. De forma a garantir a aderência aos padrões brasileiros e internacionais técnicos e de segurança, os materiais a serem fornecidos, bem como os serviços prestados, deverão estar em conformidade com as normas técnicas vigentes e com suas respectivas alterações e atualizações, especialmente as relacionadas a seguir:

8.1.1.1. ABNT NBR 5410: Estabelece as condições a que devem satisfazer as instalações elétricas de baixa tensão, a fim de garantir a segurança de pessoas e animais, o funcionamento adequado da instalação e a conservação dos bens.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.1.1.2. ABNT NBR 14.565: Especifica um sistema de cabeamento estruturado para uso nas dependências de um único ou um conjunto de edifícios comerciais em um campus, bem como para a infraestrutura de cabeamento estruturado de datacenters. Ela contempla os cabeamentos metálico e óptico.
- 8.1.1.3. ABNT NBR 14.566: Especifica os requisitos mínimos exigíveis na fabricação dos cabos ópticos dielétricos, para aplicação subterrânea em duto e aérea espinados.
- 8.1.1.4. ABNT NBR 15.465: Fixa os requisitos de desempenho para eletrodutos plásticos rígidos (até DN 110) ou flexíveis (até DN 40), de seção circular, podendo estes estar embutidos, enterrados ou aparentes, a serem empregados em instalações elétricas de edificações alimentadas sob uma tensão nominal igual ou inferior a 1.000 V em corrente alternada, com frequências inferiores a 400 Hz, ou a 1.500 V em corrente contínua. Os eletrodutos objetos desta norma também devem ser utilizados em linhas de sinal (telefonia, TV a cabo etc.).
- 8.1.1.5. ABNT NBR ISO/IEC-17.799: Estabelece as diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.
- 8.1.1.6. ANSI/EIA/TIA-606-A: Administration Standard for Commercial Telecommunications Infrastructure (Padrões para Administração em Infraestrutura de Telecomunicações Comerciais).
- 8.1.1.7. ANSI/EIA/TIA-942: Telecommunications Infrastructure Standard for Data Center (Infraestrutura de Telecomunicações para Datacenters).
- 8.1.1.8. ANSI/TIA/EIA-569-B: Commercial Building Standard for Telecommunications Pathways and Spaces (Construção e projeto dentro e entre prédios comerciais, relativas à infraestrutura de telecomunicações).
- 8.1.1.9. ANSI/TIA-568-C.0: Generic Telecommunications Cabling for Customer Premises (Cabeamento de telecomunicações genérico para as dependências do cliente).
- 8.1.1.10. ANSI/TIA-568-C.1: Commercial Building Telecommunications Cabling Standard (Cabeamento de telecomunicações para edifícios comerciais).
- 8.1.1.11. ANSI/TIA-569-C.2: Balanced Twisted-Pair Telecommunication Cabling and Components Standard (Cabeamento de telecomunicações em par balanceado e componentes).
- 8.1.1.12. EIA 310D: Cabinets, Racks, Panels, and Associated Equipment (Gabinetes, Racks, Painéis e Equipamentos Associados). ISO/IEC 11.801: Information

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Technology: generic cabling (Tecnologia da Informação: cabeamento genérico).

- 8.1.1.13. J-STD-607A: Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications (Aterramento para edifício comercial e requerimentos de conexões para telecomunicação).
  - 8.1.1.14. MTE – NR N° 1: Segurança do Trabalho – Disposições Gerais.
  - 8.1.1.15. MTE – NR N° 2: Segurança do Trabalho – Inspeção Prévia.
  - 8.1.1.16. MTE – NR N° 26: Sinalização de Segurança.
  - 8.1.1.17. MTE – NR N° 6: Equipamentos de Proteção Individual – EPI.
  - 8.1.1.18. MTE – NR N° 10: Segurança em Instalações e Serviços em Eletricidade.
  - 8.1.1.19. MTE–NR N° 11: Transporte, Movimentação, Armazenagem e manuseio de Materiais.
  - 8.1.1.20. MTE–NR N° 35: Estabelece os requisitos mínimos e as medidas de proteção para o trabalho em altura, envolvendo o planejamento, a organização e a execução.
- 8.1.2. Resolução Anatel n° 242, de 30 de novembro de 2000 da Agência Nacional de Telecomunicações – ANATEL, que garante conformidade de funcionamento no Brasil através de processo de Certificação e Homologação de Produtos para Telecomunicações para uso no território nacional.

## **8.2. RACK INTELIGENTE**

- 8.2.1. Por RACK INTELIGENTE, entende-se hardware e softwares integrados que em conjunto com proposta tecnológica capaz de fornecer uma infraestrutura com energia ininterrupta, climatização, monitoramento e controle de acesso.
- 8.2.2. O RACK INTELIGENTE deverá ser fornecido em gabinete unitário selado e autoportante, para aplicação em ambiente interno abrigado.
- 8.2.3. Deverá prover sistemas e subsistemas integrados e preparados para completa infraestrutura de missão crítica ao datacenter, incluindo energia Ininterrupta, gerenciamento térmico (ar-condicionado, corredor frio e corredor quente internos ao gabinete, e ventiladores/exaustores de emergência), gabinete/rack, distribuição de energia, monitoramento ambiental e gerenciamento/supervisionamento de infraestrutura, bem como sistema de proteção e combate à incêndio.
- 8.2.4. Deverá ser pré-fabricada e testada em fábrica como um sistema em sua totalidade, garantindo a compatibilidade entre todos os seus componentes, provendo no

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

mínimo:

- 8.2.5. Deverá suportar máxima carga de TI conectada de 3kW.
- 8.2.6. Deverá possuir no mínimo 26 U's disponíveis para montagem de equipamentos do usuário.
- 8.2.7. Cabos de dados, cabos de energia e conexões dos sensores, internos ao gabinete, devem ser pré-configurados em fábrica acomodados em infraestrutura própria para proteção física.
- 8.2.8. Tubulação entre Evaporadora e Condensadora (caso necessário) a ser executada durante a instalação e comissionamento.
- 8.2.9. O sistema de climatização não deverá rejeitar calor no mesmo ambiente físico do gabinete, devendo ser previsto condensador externo ou sistema de exaustão de dutos.
- 8.2.10. O gabinete não deverá ultrapassar a largura de 900mm, profundidade de 1400mm e altura de 2100mm, com todos os componentes montados e acoplados.
- 8.2.11. Deverá ter sistema de iluminação LED.
- 8.2.12. Nível de Ruído do gabinete menor que 58dB.
- 8.2.13. Tensão de funcionamento 220V (FNT) ou 127 (FNT), sendo permitido o uso de transformadores, para rebaixamento ou elevação da tensão.
- 8.2.14. O RACK INTELIGENTE deverá possuir Altura máxima 2000mm, 42U, largura mínima 800mm e máxima de 900mm e Profundidade máxima 1400mm.
- 8.2.15. Profundidade Disponível para montagem de equipamentos mínima de 740mm.
- 8.2.16. Profundidade do corredor frio dentro do gabinete de no mínimo 19mm.
- 8.2.17. Profundidade do corredor quente dentro do gabinete de no mínimo 19mm.
- 8.2.18. Norma de Instalação de Equipamentos - 19", EIA-310-D.
- 8.2.19. Capacidade Estática de Suporte a Carga de no mínimo 1000kg
- 8.2.20. Cor preferencialmente preta.
- 8.2.21. Portas traseiras e dianteiras isoladas com vidro selado ou policarbonato transparente, com fechaduras escamoteáveis e chaves com o mesmo segredo, com abertura mínima de 95°.
- 8.2.22. Possuir área de Acesso frontal e traseira e painel lateral removível.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.2.23. Deverá suportar a instalação 2 réguas de energia vertical (RPDU - padrão 0U).
- 8.2.24. Deverá ser fornecido no mínimo 10 painéis cegos por rack na mesma cor do rack para instalação e ocupação em 1U de altura em racks 19” EIA-310-D, sua montagem deverá ser sem o uso de ferramentas (“tool-less”).
- 8.2.25. Deverá ser fornecido sistema de ventilação/exaustão compatíveis com rack de 42UA, com tensão nominal de 220volts e conectado ao sistema de energia crítica do RACK INTELIGENTE, seu nível de ruído máximo admissível de 65dbA
- 8.2.26. Deverá possuir no mínimo 2 ventiladores que auxiliam a retirada de ar quente do rack.
- 8.2.27. Deverá ser fornecido réguas elétrica monitoráveis(PDU) zero U, com tensão nominal de entrada de 220V, frequência de 60Hz, suportar tensão de entrada aceitável de 220-240V AC, corrente nominal de funcionamento de 32ª e possuir tipo de conexão de entrada IEC-C20.
- 8.2.28. As PDU gerenciáveis deverão possuir tensão nominal de saída de 220V, corrente nominal de funcionamento de 16A, possuir no mínimo 24(vinte e quatro) tomadas, sendo 18(dezoito) padrão IEC-320-C13 e 6(seis) IEC-320-C19, deverá possuir proteção contra sobrecarga.
- 8.2.29. Deverá possuir monitoramento das condições de funcionamento, da régua como um todo, com aferição de no mínimo as seguintes grandezas: tensão (V), potência (kW) e corrente elétrica (A).
- 8.2.30. Deverá possuir monitor digital para monitoramento local de no mínimo as grandezas de tensão (V) e corrente elétrica (A).
- 8.2.31. Deverá possibilitar integração com sistema de supervisão do RACK INTELIGENTE, via protocolo MODBUS RS485 ou via SNMP ou via Private Protocol, para finalidade de monitoramento remoto via interface web.
- 8.2.32. Deverá ter a função de gerenciamento, tomada a tomada, sendo esta função a capacidade de ligar e desligar a energia o de cada tomada, localmente e remotamente via interface de gerenciamento.
- 8.2.33. Deverá ser fornecido sistema de energia ininterrupta – UPS, possuindo tecnologia Dupla Conversão, True on Line, com retificador e inversor ambos dotados de funcionamento com IGBT.
- 8.2.34. O sistema de UPS deverá ser composto de retificador/carregador de baterias independente, inversor, chave estática, bypass de manutenção interno, e ter cada um seu próprio banco de baterias, que não poderá ser ligado diretamente ao barramento DC quando em operação dentro da faixa de aceitação da tensão de

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

entrada, não podendo estar sujeito a ripple de tensão em seus terminais e de forma a otimizar seu prazo de vida útil.

- 8.2.35. A UPS deverá ter potência mínima de 6kVA / 6kW e possuir baterias internas e possibilite a inclusão de módulos externos de baterias, de forma modular acrescer módulos adicionais para aumento de autonomia.
- 8.2.36. O sistema UPS deverá possuir frequência nominal de entrada nominal de 60 Hz, com variação de 40 Hz ~ 70 Hz, tolerância da tensão de entrada ajustável entre 176 Volts ~ 280 Volts (monofásica - FNT).
- 8.2.37. O sistema UPS deverá possuir eficiência AC-AC de no mínimo 94%, possuir tipo de conexão de entrada com Borne 3 fios F-N-T, FP de entrada > 0,99.
- 8.2.38. O sistema UPS deverá possuir proteção de regulação de frequência e tensão, proteção de cargas conectadas contra surtos, picos e outros distúrbios elétricos. Distorção harmônica de corrente:  $\leq 3\%$  para plena carga linear e  $\leq 5\%$  for para plena carga não linear.
- 8.2.39. Partida a Frio: Permite ligar o no-break para fornecer energia temporária de emergência mesmo quando não há energia elétrica.
- 8.2.40. Deverá possuir proteções contra sobrecarga e surtos de tensão.
- 8.2.41. Deverá possuir reinício automático no caso de restabelecimento de energia elétrica após a descarga das baterias.
- 8.2.42. O sistema UPS deverá possuir capacidade mínima de Potência Nominal Ativa de 6000 Watts de saída.
- 8.2.43. Deverá possuir capacidade mínima de Potência Nominal Aparente de 6000 Volt Ampere.
- 8.2.44. Deverá possuir tensão nominal de saída de 220 Volts (monofásica - FNT).
- 8.2.45. Deverá possuir Frequência de saída (sincronizada com rede elétrica) de 60Hz nominal, com estabilidade de  $\pm 3,5\text{Hz}$ .
- 8.2.46. Deverá possuir fator de crista de 3:1.
- 8.2.47. Fator de potência de saída unitário (FP=1).
- 8.2.48. Deverá possuir forma de onda na saída senoidal pura com Dupla Conversão, não sendo aceitas formas de ondas modificadas.
- 8.2.49. Deverá possuir distorção da tensão de saída  $\leq 2\%$  para cargas lineares e  $\leq 5\%$  para cargas não lineares.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.2.50. Deverá possuir tipo de conexão de saída com Borne 3 fios F-N-T.
- 8.2.51. Deverá suportar Sobrecarga de:
- 0 <105%, contínuo;
  - 1 105% até 125% , 5 minutos;
  - 2 125% até 150%, 60 segundos;
  - 3 >150%, por no mínimo 200ms;
- 8.2.52. O sistema UPS deverá possuir um painel de controle com display de cristais líquidos retro iluminados, que poderá exibir diagramas gráficos e símbolos para monitoramento e controle total do UPS.
- 8.2.53. A unidade UPS deverá possuir capacidade de ser instalado em rack do padrão 19”.
- 8.2.54. A unidade de UPS deverá possuir, internamente, seccionadoras para manobras, referentes à entrada do retificador, banco de baterias, à entrada da alimentação reserva (by-pass), ao by-pass mecânico de manutenção e saída para carga.
- 8.2.55. O Sistema UPS deverá possuir gerenciamento remoto, via browser através de porta ethernet no equipamento, possuir interfaces USB, SNMP e Modbus, deverá se comunicar com o sistema de supervisão do RACK INTELIGENTE, para finalidade de monitoramento e gerenciamento.
- 8.2.56. A unidade UPS deverá possuir altura máxima de 5U e suportar a montagem em rack de 19”.
- 8.2.57. O sistema UPS deverá possuir Temperatura de operação de 0 a 40°C, deverá possuir Umidade de operação de 5 a 95% sem condensação e deverá possuir Alarmes Visual e Sonoro.
- 8.2.58. O sistema UPS deverá possuir documentação técnica necessária (manual de usuário) a instalação, configuração, operação e verificação das propostas e deverá ter as seguintes conformidades com normas e padrão de uso:
- 0 Segurança: IEC62040-1:2008 versão, GS mark
  - 1 EMI/EMC/C-Tick EMC: IEC/EN/AS 62040-2 2nd Ed (Cat 2)
  - 2 ESD IEC/EN: EN61000-4-2, nível 4, Criterio A
  - 3 Radiação: IEC/EN EN61000-4-3, nível 3, Criterio A
  - 4 Transientes elétricos: IEC/EN EN61000-4-4, nível 1 4, Criterio A
  - 5 Imunidade contra surtor IEC/EN EN61000-4-5, nível 3, Criterio A
  - 6 Compliance CE
- 8.2.59. Deverá possuir Baterias V.R.L.A (Valve Regulated Lead Acid) - Chumbo-Ácido selada regulada por válvula, livre de manutenção, a prova de vazamento, própria para uso em equipamentos do tipo UPS. Não será aceito equipamento com uso de

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

bateria do tipo automotiva ou similar.

- 8.2.60. As baterias deverão ser acondicionadas internamente ao gabinete do UPS.
- 8.2.61. Deverá energizar o equipamento com partida a frio, somente pelas baterias.
- 8.2.62. Deverá possuir autonomia mínima de 10 minutos, para carga de 3kW.
- 8.2.63. Deverá possuir capacidade expansível para adição de mais módulos de baterias externas.
- 8.2.64. Os módulos externos de bateria deverão possuir gabinete compatível com o mesmo tipo de fabricação e modelo de UPS;
- 8.2.65. O RACK INTELIGENTE deverá ser fornecido com painel elétrico para montagem em rack de 19" (rack mount).
- 8.2.66. O painel de alimentação elétrica deverá receber o circuito alimentador do RACK INTELIGENTE, com conexão ao Disjuntor Geral de Alimentação do Painel.
- 8.2.67. O painel de alimentação elétrica deverá prover alimentação elétrica (a montante) para: UPS e equipamento refrigeração de precisão. Deverá ser previsto Disjuntor Geral de Alimentação e disjuntores parciais para proteção e seccionamento dos circuitos alimentadores de cada equipamento citado neste item, corretamente dimensionados.
- 8.2.68. Deverão ser previstos disjuntores para a realização de Bypass do UPS, para quesitos de manutenção corretamente dimensionados.
- 8.2.69. Deverá prover distribuição elétrica a jusante do UPS para: ventiladores de emergência conectados ao UPS, Racks PDU Monitoráveis, Console de Monitoramento Ambiental e Supervisão do RACK INTELIGENTE, Iluminação tipo LED e display frontal. Deverá ser previsto Disjuntor Geral de Distribuição do UPS e serem previstos disjuntores parciais para proteção e seccionamento dos circuitos de alimentação de cada equipamento citado neste item, corretamente dimensionados.
- 8.2.70. O RACK INTELIGENTE deverá prover sistema de ar condicionado de precisão com potência mínima de 3500W
- 8.2.71. A unidade ar-condicionado de precisão deverá ofertar às cargas de TI dos usuários, 3000W de potência de climatização.
- 8.2.72. A unidade ar-condicionado de precisão deverá ser capaz de suportar a carga térmica do UPS além da oferta de climatização da carga de TI dos usuários.
- 8.2.73. Metodologia de Refrigeração: expansão direta a ar, controle de precisão, com variação de potência de climatização ofertada de 900W a 3000W e controle

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

variável dos ventiladores da evaporadora.

- 8.2.74. A unidade ar-condicionado de precisão deverá ser posicionada na parte inferior do gabinete de 19” ou acoplado lateralmente ao gabinete de 19”.
- 8.2.75. A unidade ar-condicionado de precisão deve possuir tensão de Entrada: 220V (FNT), frequência de 60hz com capacidade de mínima de refrigeração: 3,5kW.
- 8.2.76. A unidade ar-condicionado de precisão, deverá usar gás Refrigerante do Tipo R410A.
- 8.2.77. Evaporadoras com uso de ventiladores de capacidade variável: EC Fan.
- 8.2.78. Condensadora externa ou condensadora integrada (com rede dutos acoplados para exaustão do calor).
- 8.2.79. Sentido do Fluxo de Ar Interno sendo da traseira (corredor quente) para frente (corredor frio).
- 8.2.80. O RACK INTELIGENTE deverá possuir uma plataforma escalável de monitoramento ambiental e supervisão dos componentes de forma integrada, que permitirá realizar o monitoramento de sensores ambientais e supervisão dos dispositivos em tempo real e apresentar notificações imediatas de problemas.
- 8.2.81. Deverá possibilitar o controle e gerenciamento remotos por interface web (https), sendo possível por intermédio dessa interface.
- 8.2.82. Deverá possibilitar o controle e gerenciamento local por interface homem máquina – IHM: LCD touchscreen de no mínimo 7 polegadas
- 8.2.83. Deverá se conectar e monitorar os sistemas de energia e refrigeração via protocolos e sensores via SNMP ou MODBUS RS485 ou slot inteligente na UPS.
- 8.2.84. Deverá possibilitar a visualização de todos os parâmetros disponíveis, ambientais e de funcionamento dos componentes monitoráveis em telas gráficas via interface web e display de LCD acoplado ao gabinete.
- 8.2.85. Deverá ter integrado os seguintes sensores: 2 (dois) sensores de temperatura, 2 (dois) sensores de abertura de porta de rack de 19” e 1 (um) sensor de detecção de líquido.
- 8.2.86. Deverá suportar a inclusão de Modem SMS, para instalação futura.
- 8.2.87. Deverá possibilitar o monitoramento de Alarmes e e envio de alertas via e-mails e SMS.
- 8.2.88. Deverá permitir a Integração com BMS e outros sistemas de supervisão via protocolo SNMP.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.2.89. Deverá ser fornecido com sistema de controle de acesso para as portas: dianteira e traseira. O sistema deverá ser composto de fechaduras eletromagnéticas para as portas dos racks com controle através de cartão de proximidade local e possibilidade de abertura remota via interface web de gerenciamento. Deverá ser integrado ao monitoramento centralizado deste item, com a possibilidade de registrar de forma inteligente eventos do histórico de controle de acesso, produzir um alarme para o tempo limite da porta não fechada; e suportar a abertura remota de portas.
- 8.2.90. Deverá ser fornecido com uma câmera de vídeo vigilância de rota única (câmera IP - IPC) específica para o gabinete/rack; devendo ser integrada ao sistema de gerenciamento centralizado e realizar o monitoramento em tempo real e salvamento de imagens, via sistema de gerenciamento, sempre que acionado algum alarme configurado na plataforma de supervisão centralizada.
- 8.2.91. Deverá proporcionar entrega de gerenciamento e monitoramento do RACK INTELIGENTE em tempo real de toda a infraestrutura de crítica, incluindo, mas não se limitando a, unidades de distribuição de energia, (PDU), fontes de alimentação (UPS), monitoramento ambiental.
- 8.2.92. Deverá ser disponibilizado em arquitetura baseada e projetada em padrões abertos de tecnologia web, o acesso à aplicação deve ser por meio de navegadores web, compreendendo no mínimo:
- Microsoft Edge
  - Mozilla Firefox
  - Google Chrome
- 8.2.93. O software contido deverá fornecer:
- Acesso de usuários simultâneos ilimitados
  - Base de dados histórica
  - Suportar integração com dispositivos de terceiros
  - Suportar Open Restful e OBIX API
- 8.2.94. A interface gráfica de usuário(GUI) deverá prover no mínimo painéis para exibição de gráficos, alarmes/eventos, controle de gráficos ativos, menus para acesso de operações, análises e relatórios de ações para os eventos.
- 8.2.95. A interface GUI da estação de trabalho deverá permitir a exibição de gráficos em 1920x1080 pixels e 32-bit true color.
- 8.2.96. O software deverá apresentar as localizações das infraestruturas gerenciadas relacionadas à pontos locais demarcados.
- 8.2.97. Os gráficos de gerenciamento deveram mostrar os componentes por meio de representação gráfica (pontos, status de cores, rótulos, etc.). Deve permitir que os

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

dispositivos SNMP possam ser integrados através da interface web do usuário final.

O equipamento visualizado deverá mostrar o seu status com no mínimo PDU do rack monitorado, UPS e assim por diante.

Deverá permitir que os usuários possam navegar pelos alarmes e informações dos equipamentos em detalhes completos, incluindo o status individual de todos os dispositivos associados.

8.2.98. Deverá permitir que as telas de visualizações de sites possam ser customizadas pelo usuário.

8.2.99. O sistema gráfico deverá permitir a visualização de cada parte do equipamento monitorado, ou controlado por:

Cada edifício

Cada andar

Cada sala

Cada rack

Cada dispositivo

8.2.100. Deverá associar eventos e alarmes à um sistema, área ou equipamento específico em que deverão ser exibidos na visualização do site principal, ou em console de alarmes embutido. Deve ter a capacidade nativa para alarmar em todos os dispositivos conectados. O sistema de alarme deve ter vários tipos de alarme, dependendo do nível de gravidade. Os usuários devem ser capazes de pesquisar pelas telas de visualizações para localizar as fontes de alarmes. Eventos, alarmes e relatórios de ações devem ter os seguintes recursos:

Capacidade de exibir as seguintes informações para cada alarme que ocorreu no sistema: Estado do Alarme (com a cor do status associada), Local, Dispositivo, Circuito, Tenant, Ponto, Tipo de Ponto, Unidade de Ponto, Fonte, Último Alarme, Confirmação solicitada, Estado de confirmação, Última confirmação, Última ação reconhecida por, Último retorno ao normal, Última atualização, Classe de alarme, Classe de aviso, Mensagem e notas. O console de alarme também deve fornecer um link para o local, dispositivo e ponto.

Os usuários devem ser capazes de escolher os limites (alto e baixo) para quando um alarme e / ou aviso será ativado, junto com os pontos para o nível de gravidade. Os usuários devem ser capazes de reconhecer e filtrar alarmes. Os alarmes devem priorizar os alarmes mais importantes. Deve incluir uma página de histórico de alarme onde todos os alarmes do sistema são armazenados. Os usuários devem ser capazes de pesquisar alarmes anteriores por local, dispositivo ou ponto.

8.2.101. Deve ser capaz de notificar diferentes usuários com base no tipo de alarme. Os usuários devem ser capazes de reconhecer alarmes remotamente. O sistema de alarme deve ser capaz de notificar os usuários até que uma pessoa reconheça o

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

alarme por meio de níveis crescentes de alarme. O sistema de alarme deve ser capaz de alertar os usuários por e-mail. Deve permitir que os usuários personalizem as mensagens de alarme por nível de escalonamento. Instruções de alarme exclusivas devem estar disponíveis no sistema. Os usuários devem ser capazes de editar mensagens para alarmes e retornar ao status normal. O usuário deve ser capaz de:

Visualizar eventos em todo o sistema.

Dependendo do nível de acesso, gerencie o evento por meio de confirmações, exclusões, regras de classificação e visualização de notas de alarme.

Configurar notificações de alarme / evento:

Console de alarme e janela pop-up de alarme o  
E-mail

8.2.102. Deverá permitir a configuração do controle de acesso por meio de usuário e senha.

8.2.103. Deverá permitir que os administradores definam o nível de acesso para diferentes usuários, as permissões devem incluir no mínimo as seguintes opções:

Leitura / Gravação: Acesso total de leitura e acesso total de gravação a todo o sistema.

Somente leitura: Acesso de leitura total, mas nenhuma gravação ou alteração pode ser feita.

Leitura / Reconhecimento: Leitura completa, mas nenhuma gravação ou alterações podem ser feitas, exceto para o banco de dados de alarmes para reconhecimento de alarmes. O administrador do sistema deve ter a capacidade de atribuir combinações de funções e privilégios aos usuários.

8.2.104. Deverá possuir a funcionalidade de registro de log para registrar as atividades do operador e algumas atividades do sistema, como abrir e fechar o banco de dados ou exclusões automáticas.

8.2.105. O operador deve ter a capacidade de visualizar tendências com um gráfico de linha de série temporal usando o banco de dados de histórico ou selecionando um ponto específico na GUI. O gráfico de linha deve ser exportável dentro da janela pop-up para o Microsoft Excel e pode ser salvo como uma visualização para ser usada em ferramentas analíticas.

8.2.106. Os dados de tendências devem ser coletados localmente e retidos no disco rígido local.

8.2.107. Os registros históricos devem ser salvo para corresponder ao intervalo de sondagem definido pelo usuário. Cada ponto de tendência deve ter a capacidade de ser tendido em um intervalo exclusivo, conforme especificado pelo usuário.

8.2.108. O usuário deve ser capaz de inserir um valor para a tolerância (mudança de valor) se os dados do ponto mudarem pelo valor especificado entre as leituras históricas, um registro separado será criado.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.2.109. Deve ser possível passar o mouse sobre qualquer valor em um gráfico de histórico e ter o valor numérico e a hora da captura de dados exibidos.
- 8.2.110. Qualquer ponto de tendência no sistema pode ser avaliado juntamente com qualquer outro ponto de tendência no sistema. Unidade ou local não deve definir tendências.
- 8.2.111. Os valores de tendência podem ser apresentados em formato gráfico de gráfico de linha.
- 8.2.112. O sistema deve ter a capacidade de executar uma mudança de parâmetro global (por exemplo, configuração em massa de todos os pontos ou um subconjunto filtrado de pontos para tendência histórica e / ou pontos de ajuste de alarme).
- 8.2.113. O software deve permitir aos usuários visualizar relatórios criados anteriormente, bem como criar novos relatórios definidos pelo usuário.
- 8.2.114. Os relatórios devem conter visualizações utilizando os seguintes tipos de gráficos:

- Gráfico de barras
- Medidor
- Gráfico de pizza
- Gráfico de dispersão
- Valor Simples
- Mesa
- Série Temporal
- Imagem do usuário
- Texto do usuário

- 8.2.115. Os relatórios definidos pelo usuário devem incluir, mas não se limitar a:

- Alarmes
- Dados históricos do dispositivo
- Dados de tendência com base no período de tempo definido pelo usuário
- Cada relatório deve poder ser salvo eletronicamente. Os relatórios padrão e definidos pelo usuário podem ser salvos nos seguintes formatos de arquivo:
  - XLS
  - PDF
- Cada relatório deve ter a capacidade de ser entregue por e-mail ou salvo em um caminho de arquivo especificado, usando uma programação diária / semanal / mensal.

- 8.2.116. O DCIM deve fornecer ferramentas de gerenciamento de rack de TI e conter os seguintes recursos:

- Visualização do rack de TI, onde o usuário pode pesquisar racks de TI por nome, marca, modelo, número de série, etiqueta de ativo e assim por diante.
- O usuário deve ser capaz de associar dados de energia e ambientais a cada

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

rack.

Outras informações importantes do rack, como localização do rack, RU usado e RU livre (dianteiro e traseiro), detalhes de contato, etc. - junto com a capacidade de selecionar / desmarcar colunas na visualização.

O usuário também deve ser capaz de criar colunas personalizadas para inserir dados personalizados.

Deve permitir que os usuários adicionem novos racks ao sistema e exportem / importem dados do rack usando o formato de planilha, para incluir a instalação de ativos de TI dentro do rack.

O usuário deve ser capaz de se conectar à visualização individual do rack a partir do banco de dados do rack principal.

8.2.117. O DCIM deve fornecer a capacidade de controlar pontos via SNMP, junto com a capacidade do usuário criar grupos de controle. Os grupos de controle consistirão em pontos idênticos em todo o equipamento (único ou múltiplo) que podem receber um comando de controle para todo o grupo.

8.2.118. O DCIM deve fornecer aos usuários um recurso para gerenciar eventos de manutenção de dispositivo. O recurso de manutenção silenciará todos os alarmes e tendências em equipamentos específicos ou vários equipamentos durante o evento de manutenção.

Os usuários devem ser capazes de colocar um dispositivo no modo de manutenção instantaneamente ou programar a manutenção dentro da interface, para um ou vários dispositivos agrupados ao mesmo tempo.

Os usuários têm a opção de receber notificação por e-mail para o início e o fim dos eventos de manutenção.

Os eventos de manutenção devem incluir datas de início e término, dispositivos e descrições de tarefas.

Os usuários devem ser capazes de visualizar o histórico de manutenção.

Deve permitir aos usuários adicionar, editar e excluir tarefas de manutenção. Os eventos concluídos não podem ser excluídos.

8.2.119. O software deve oferecer suporte à integração de software por meio de sua API aberta.

8.2.120. O software também estará sujeito às políticas da CONTRATANTE para segurança, sem efeito na operação do Servidor ou Cliente.

8.2.121. O sistema não deve implantar protocolos inerentemente suscetíveis a intrusão.

8.2.122. O sistema deve retirar todos os arquivos e serviços desnecessários do serviço da Web para proteger a CONTRATANTE de intrusões.

8.2.123. O software deve suportar os seguintes bancos de dados, no mínimo:

a) MySQL

8.2.124. Todos os componentes do software devem ser instalados e concluídos de acordo

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
com a especificação. Os componentes devem incluir:

Software de servidor, banco de dados e interface gráfica do usuário do navegador da Web.

Utilitários de configuração do sistema para futuras modificações no sistema.

- 8.2.125. O RACK INTELIGENTE deverá contar com sistema de proteção e combate à incêndio do tipo modular para proteção de um volume de até 3m<sup>3</sup> e operar de forma autônoma, automática e sem intervenção humana.
- 8.2.126. O sistema de combate à incêndio deverá ser composto de no mínimo dois detectores pontual de fumaça operando de forma cruzada, permitir acesso remoto via TCP/IP e interligar com sistema monitoramento ambiental, através de protocolos abertos: MODBUS, BACNET, SNMP e ou Relês de Contato (NA / NF). O agente de extinção deverá ser o FK-5-1-12, listado na NFPA 2001.
- 8.2.127. O sistema de supressão automático com a aplicação de gás deverá atuar por inundação completa do ambiente enclausurado dos RACKS AUTÔNOMOS com o gás inerte, em volume recomendado pelas normas, para o ambiente.
- 8.2.128. O sistema deve atender a norma Americana NFPA 2001. O equipamento deverá ter aprovação UL ou equivalente. Sendo que cada módulo deverá prover proteção para até 3m<sup>3</sup>
- 8.2.129. Além da descarga automática deverá possibilitar acionamento manual e dispositivo que permite o bloqueio do processo de contagem (temporização) em curso para difusão do gás.
- 8.2.130. O sistema deve ser acionado automaticamente por um laço de detectores de fumaça interligados a um servidor de controle central para estes RACKS AUTÔNOMOS.
- 8.2.131. Este controle deverá ter chaveadores para bloquear a descarga de gás e o acionamento manual, e conter ainda um temporizador e sinalizadores áudios visuais dentro e fora da sala.
- 8.2.132. Características mínimas que o equipamento deverá conter:

Dimensões mínimas externas: (CxLxA),460x490x90mm(2Us)

Peso máximo: 30Kg.

Possuir até 2 (dois) cilindros com gás FK-5-1-12 com pressostato de baixa pressão.

Detector de fumaça ou temperatura.

e) Interface TCP/IP, BACNET, MODBUS e SNMP.

Permite interligação em cascata, adotando o conceito principal e secundário.

Permite instalar periféricos externos do tipo: Sirene, Detector e Acionador.

Controle e monitoramento local e remoto, via web browser ou app.

4 zonas de detecção independentes, operando de forma cruzada.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Níveis de acesso para operação, testes e configuração.

Display de LCD – 5 linhas.

Bateria interna. Stand-by 24h – Alarme 15min.

Relé Alarme/Falha. 50Vdc@5Amp.

Alimentação elétrica. Bivolt 230V/110V @ 10A (1.1KVA).

Buzzer interno de aviso.

p) Sistema supressão baixa pressão. 240 psi – 16,5 bar.

Conforme normas EN54-2, EN54-4 e EN 12094-1.

Tempo de pré-alarmede combate programável.

Indicadores de alarme / falha visual.

Capacidade para proteger racks servidores/ telecomunicações com um volume de até 3,0m<sup>3</sup>.

### **8.3. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE RACK INTELIGENTE**

8.3.1. O Serviço de instalação de rack inteligente compreende todos os procedimentos necessários para tornar rack em estado operacional, incluindo as seguintes atividades:

#### **8.3.2. INSTALAÇÃO, ESTUDO E DIMENSIONAMENTO DO LOCAL DE INSTALAÇÃO DO RACK INTELIGENTE**

8.3.2.1. Compreende vistoria do local indicado pelo CONTRATANTE para instalação do RACK INTELIGENTE.

8.3.2.2. Levantamento das condições físicas do local de instalação, incluindo: aferição do espaço físico para alocação do RACK INTELIGENTE (LarguraxComprimentoxAltura) m; verificação do ponto de derivação para alimentação elétrica do RACK INTELIGENTE, com confirmação das condições de fornecimento de energia para o sistema e levantamento das distancias entre ponto de alimentação e o RACK INTELIGENTE; verificação do local de instalação da condensadora remota externa, com levantamento da distância entre evaporadora e condensadora; levantamento das condições de transporte horizontal e vertical do RACK INTELIGENTE e componentes até o local de instalação; registro fotográfico de todos os ambientes vistoriados.

8.3.2.3. Confeção de relatório de vistoria com indicação e análise dos ambientes físicos e condições de instalação, incluindo relatório fotográfico dos ambientes. Deverá indicar no relatório as condições de instalação e emitir laudo de validação ou reprovação do local de instalação indicado pela CONTRATANTE, com sustentação técnica da decisão por parte COTRATADA.

8.3.2.4. Preparação de projeto executivo da instalação do RACK INTELIGENTE, contemplando no mínimo: Layout do ambiente de instalação com indicação do RACK INTELIGENTE no local de instalação em prancha de projeto; diagrama unifilar das instalações; desenho isométrico das instalações dos climatizadores de precisão, indicando distâncias verticais e horizontais.

8.3.2.5. Emissão de ART de projeto pelo responsável técnico da CONTRATADA.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.3.2.6. Confecção do DATABOOK do sistema do RACK INTELIGENTE, contemplando todos os manuais de instalação e operação de todos os subsistemas.

8.3.3. SERVIÇO DE INSTALAÇÃO ELÉTRICA DO RACK INTELIGENTE

- 8.3.3.1. Preparação do ponto de derivação da alimentação elétrica do RACK INTELIGENTE, com a instalação de disjuntor de derivação em painel elétrico indicado como ponto de derivação, na infraestrutura existente no local de instalação, corretamente dimensionado em conformidade com o projeto executivo a ser apresentado ao CONTRATANTE.
- 8.3.3.2. Instalação do circuito alimentador do RACK INTELIGENTE, corretamente dimensionado, em conformidade ao projeto executivo a ser apresentado a CONTRATANTE e NBR 5410. Deverá ser considerada infraestrutura de acomodação e proteção física do circuito em eletrocalhas metálicas, em conformidade com NBR 5410. Deverá ser considerada a conectorização do circuito no disjuntor de alimentação geral, como também a conectorização do circuito ao disjuntor geral do RACK INTELIGENTE (no painel de alimentação do RACK INTELIGENTE)
- 8.3.3.3. O lance de cabos entre o ponto de derivação da alimentação do RACK INTELIGENTE e o RACK INTELIGENTE, não deverá ser superior a 40 metros, para quesitos de precificação

8.3.4. SERVIÇO DE INSTALAÇÃO DE REDE FRIGORÍGENA DO RACK INTELIGENTE

- 8.3.4.1. Instalação das condensadoras por traslado de sua(s) unidade(s) e ao local de instalação, posicionamento físico sobre suporte de fixação com calços antivibrante.
- 8.3.4.2. Composição de linhas frigorígenas, corretamente dimensionadas, em consonância com os requisitos indicados pelo fabricante e projeto executivo.
- 8.3.4.3. Rede frigorígena deverá ser em tubos de cobre sem costura, parede dupla, com distância linear máxima de 15 (quinze) metros de linha equivalente entre o conjunto evaporadora-condensadora. Os suportes e ancoramento das tubulações, no piso, teto e paredes deverão ser realizados com sistemas de canaletas metálicas, perfilados, barras rosqueadas, chumbadores parabol e fixadores de tubos em cunha cônica de aperto, tipo SRS. As linhas deverão ser isoladas com revestimento de borracha elastomérica de 19 mm de espessura, tubulações instaladas ao tempo com revestimento em lâminas de alumínio corrugado.
- 8.3.4.4. Observar a melhores práticas indicadas pelo fabricante do equipamento de climatização de precisão

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

8.3.5. SERVIÇO DE STARTUP E COMISSIONAMENTO UPS

- 8.3.5.1. Identificação das partes do sistema e execução da limpeza dos componentes e do sistema como um todo.
- 8.3.5.2. Energização inicial do conjunto de equipamentos e configurações para uso, com respeito a Norma Regulamentadora Brasileira para Trabalhos com Eletricidade NR-10.
- 8.3.5.3. Testes e ensaios dos componentes e do sistema em campo.
- 8.3.5.4. Acionamento do sistema com configurações iniciais e realização dos ensaios de aceitação do sistema.
- 8.3.5.5. Emissão do relatório de startup e comissionamento com posterior entrega ao CONTRATANTE em no máximo 10 dias úteis.
- 8.3.5.6. Fornecimento de Manuais de Uso e Operação (um por equipamento).
- 8.3.5.7. Realização de treinamento operacional, no momento da realização do startup (comissionamento), cedido a equipe técnica da CONTRATANTE, abordando a manutenção básica das unidades (verificação de logs, eventos, módulos de potência e baterias)

8.3.6. SERVIÇO DE STARTUP E COMISSIONAMENTO DO AR  
CONDICIONADO DE PRECISÃO

- 8.3.6.1. Identificação das partes do sistema e execução da limpeza dos componentes e do sistema como um todo.
- 8.3.6.2. Energização inicial do conjunto de equipamentos e configurações para uso, com respeito a Norma Regulamentadora Brasileira para Trabalhos com Eletricidade NR-10.
- 8.3.6.3. Testes e ensaios dos componentes e do sistema em campo:
- 8.3.6.4. Regulagem e balanceamento mecânico do sistema de climatização;
- 8.3.6.5. Realização da pré-operação do sistema;
- 8.3.6.6. Acionamento do sistema com configurações iniciais e realização dos ensaios de aceitação do sistema
- 8.3.6.7. Emissão do relatório de startup e comissionamento com posterior entrega ao CONTRATANTE em no máximo 10 dias úteis.
- 8.3.6.8. Fornecimento de Manuais de Uso e Operação (um por equipamento).
- 8.3.6.9. Realização de treinamento operacional, no momento da realização do startup

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
(comissionamento), cedido a equipe técnica da CONTRATANTE, abordando a manutenção básica das unidades de Evaporadoras e Condensadoras (verificação de filtro, ventiladores, dentre outras funcionalidades técnicas-operacionais).

**8.3.7. SERVIÇO DE STARTUP E COMISSIONAMENTO DA SUPERVISÃO E MONITORAMENTO DO RACK INTELIGENTE**

- 8.3.7.1. Serviços de verificação física do monitoramento ambiental com aferição da integração de dispositivos sensoriais e monitoramento.
- 8.3.7.2. Serviços de configuração dos limites de alarmes e dos sistemas de notificação por email e padrões de notificação.
- 8.3.7.3. Serviços de testes das configurações e de startup do sistema
- 8.3.7.4. Fornecimento de Manuais de Uso e Operação do sistema de monitoramento ambiental.
- 8.3.7.5. Serviços de configuração do módulo de supervisão do RACK INTELIGENTE com configuração de alertas críticos, dos sistemas de vigilância por vídeo e todo tipo de informações-chave.
- 8.3.7.6. Serviços de configuração da supervisão e controle dos dispositivos relacionados à energia crítica, refrigeração, segurança, aspectos ambientais e integrações com outros sistemas.
- 8.3.7.7. Serviços de testes das configurações e de startup do sistema de supervisão do RACK INTELIGENTE
- 8.3.7.8. Fornecimento de Manuais de Uso e Operação do sistema de supervisão do RACK INTELIGENTE

**8.4. SISTEMA UPS MODULAR DE 150 KVA/150KW**

- 8.4.1. O Serviço de instalação de sistema UPS modular de 150KVA/150KW compreende todos os procedimentos necessários para tornar o sistema de UPS operacional, incluindo as seguintes atividades e materiais:
- 8.4.2. Fornecimento de UPS modular de 150 kVA/150kW, carregados com 120/120kW KVA em módulos para carga e mais um módulo redundante, na configuração singelo 380/220V com autonomia de 7 min a uma carga de 120kW, com baterias hotswap.
- 8.4.3. Esta especificação descreve um Sistema de Energia Ininterrupta, modular com frame com capacidade expansão mínima de até 150kW, com módulos de potência hot-swappable de 16 à 30 kW, módulos de bateria hot-swappable, topologia True On-Line/Dupla Conversão, para alimentação de cargas críticas.
- 8.4.4. O Sistema UPS inicialmente deverá atender uma carga de 120kW, em, com

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
redundância interna em n+1 módulos.

8.4.5. São consideradas, minimamente as seguintes características gerais para o sistema de UPS a ser fornecido:

- a) Normas obrigatórias: IEC/EN 62040-1. IEC/EN 62040-2. IEC/EN/AS60950. IEC/EN/ AS61000. (IEC/EN/AS60146 e 60529).  
IEC62040-3 Classe 3. ISO 9001  
Refrigeração: Do tipo Forçada.  
Ventilação: Deverá ser frontal, com tomada de ar pela frente e exaustão traseira. Para traseira será previsto espaço de 60cm.  
Gabinete: Grau de Proteção IP 20 (conf IEC 60529), mesmo com porta frontal aberta.  
Eficiência: Deverá ter eficiência mínima de 95% em modo dupla- conversão, a plena carga.  
Dissipação Térmica: Num cenário de carga de 54 kW, a dissipação térmica máxima deverá ser de no máximo 3.0 kW operando em DUPLA CONVERSÃO.  
Ruído audível: Menor que 65dBA @ 90 kW medido a 1m frontal da UPS a plena carga.  
Dimensão máxima de conjunto UPS+Bateria: UPS L600xP1200xA2000mm.

8.4.6. Características mínimas da entrada (Retificador)

- Tensão de Entrada: 380/220V 3F+N+T  
Distorção THDi<5%.  
Fator de Potência de Entrada 0,98 (meia carga) e 0,99 (plena carga).  
A UPS deverá tolerar variações de 40Hz a 70Hz na entrada, mantendo 60Hz na saída do inversor, fazendo a regulação sem transferir para as baterias.  
A UPS deverá tolerar variações de 305V a 475V na entrada, mantendo 380V na saída do inversor, fazendo a regulação sem transferir para as baterias.

8.4.7. Características Mínimas de Saída (Inversor)

- Capacidade total mínima do frame: 150kW  
Capacidade instalada: 120kVA / 120kW + 30kVA/30kW (N+1)  
Fator de Potência de Saída 1 (plena carga).  
Tensão de Saída: 380V 3F+N+T  
Deverá ser IGBT / PWM  
UPS deverá suportar sobrecarga de: 125% por 10min. 150% por 1min  
THDv<1% para carga linear. <4% p/ carga não-linear conf. EN 50091-3. Fator de crista 3:1.

8.4.8. Características mínimas do Barramento DC

- a) As baterias deverão ser obrigatoriamente modulares, instaláveis e extraíveis a quente (hot-swapp).

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

A autonomia inicial mínima de cada UPS deverá ser de 7 min para carga de 54kW, @ 25°C, e considerando tensão final de descarga de 1.6V por elemento. O proponente deverá apresentar, quando solicitado, a memória de cálculos das baterias e o catálogo das mesmas, comprovando o atendimento. Os módulos (strings) de baterias deverão ser do tipo hot-swapp, com remoção da gaveta a quente pelo usuário sem bypass ou interrupção da carga, de modo que se possa colocar o “módulo” em uma bancada para substituição dos monoblocos e posterior reinserção no Gabinete UPS.

Os espaços destinados a módulos hot-swapp de baterias inicialmente vazios deverão ter tampas cegas instaladas, e serão removidas pelo usuário no ato da instalação de um novo banco de baterias hot-swappable.

**8.4.9. Características Mínimas da Chave Estática (Bypass Estático)**

Capacidade Nominal de 150kW, robusta, devendo suportar sobrecarga de 135% por longo prazo e 170% por 1 hora.

O tempo de transferência (entre bypass e inversor) síncrona deverá ser <4ms.

**8.4.10. Características Mínimas de Bypass Manual de Manutenção**

O UPS deverá ter um segundo circuito de bypass, de acionamento manual, para prover segurança ao operador durante manutenções preventivas ou corretivas, enquanto através desse circuito o UPS provê energia da Rede ou Gerador para a Carga Crítica. O BYPASS DE MANUTENÇÃO deverá permitir ativação ou desativação manual, por meio de chave ou disjuntor localizada na própria UPS. A transferência entre o BYPASS ESTÁTICO e o BYPASS DE MANUTENÇÃO deverá ser make-before-break, sem interrupção de energia para a carga crítica, e incorporada no gabinete da UPS,

fazendo parte do sistema UPS modular de 150KVA/150KW pré testado e montado em fábrica.

**8.4.11. Características mínimas do Painel de Controle do UPS**

O UPS deverá vir equipado com Display LCD amigável e intuitivo, permitindo completa monitoração e controle, com fácil visualização das informações. Deverá armazenar histórico de eventos de pelo menos 1000 registros, no idioma português ou inglês.

O microprocessador deverá controlar o display e as funções da memória do sistema de monitoração. Todas as três fases deverão ser mostradas simultaneamente. Todos os parâmetros de tensão e corrente deverão ser monitorados através de medidas RMS com precisão de  $\pm 1\%$ .

Os seguintes parâmetros deverão ser mostrados no display: Tensão de Entrada. Corrente de Entrada. Fator de Potência de Entrada. Tensão de Entrada do Bypass. Frequência de Entrada do Bypass. Tensão de saída. Corrente de saída. Fator de Potência de Saída de cada Fase. Frequência de saída. Percentual de Carga. Potência de Saída em kW e kVA de cada fase. Tensão do Barramento de Baterias. Corrente de Bateria.

**8.4.12. Características Mínimas para Monitoração Remota do UPS**

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

O sistema deverá possuir interface Web/SNMP/RJ45, para gerenciamento remoto e envio de traps para o sistema supervisorio. O fabricante deverá enviar as MIBs e prestar suporte em campo para a configuração da interface. A interface deverá ter funcionalidade de enviar, em caso de alarmes, e-mail e torpedo SMS a endereços de e-mail e telefones definidos pelo usuário. Deverá ser também fornecido como interface MODBUS RTU - RS 485 para conexão ao sistema de supervisão do DCPFM.

8.4.13. Características Mínimas dos Testes no Ambiente UPS

A CONTRATANTE poderá solicitar testes em fábrica de maneira a comprovar as características aqui solicitadas. Todos os custos serão por conta do fornecedor. Caberá à CONTRATANTE a definição de acompanhamento e realização destes testes.

O fornecedor deverá realizar treinamento operacional em campo para a equipe do cliente, demonstrando principais funções operacionais além de capacitar a equipe a instalar e remover módulos de potência ou módulos de bateria hot swap.

**8.5. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SISTEMA UPS MODULAR DE 150 KVA/150KW**

8.5.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do sistema UPS, que compreendem, entre outros, os seguintes procedimentos:

8.5.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;

8.5.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE.

8.5.4. Planejamento do local e cargas elétricas que será fornecido pelo sistema UPS;

8.5.5. Análise do posicionamento de qualquer outro equipamento ou sistema relevante;

8.5.6. Configuração do sistema de gerenciamento e monitoramento do sistema de UPS;

8.5.7. Durante a implantação sistema UPS modular de 150KVA/150KW , a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;

8.5.8. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;

8.5.9. A instalação física de todos os equipamentos (hardware) e licenças (softwares)

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE.

## **8.6. PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL**

8.6.1. Fornecimento de produto de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, compondo uma plataforma de segurança integrada e

robusta.

- 8.6.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance.
- 8.6.3. A plataforma de segurança deve possuir no mínimo a capacidade e as características abaixo, por equipamento:
- 8.6.4. Throughput de 9 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
- 8.6.5. Throughput de 4 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- 8.6.6. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;
- 8.6.7. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend);
- 8.6.8. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.
- 8.6.9. Suporte a, no mínimo, 2.800.000 conexões simultâneas;
- 8.6.10. Suporte a, no mínimo, 100.000 novas conexões por segundo;
- 8.6.11. Possuir fonte 120/240 AC ou DC, redundante e hot-swappable;
- 8.6.12. Deverá possuir Disco Solid State Drive (SSD), com no mínimo, 240 GB;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.13. Deverá possuir, no mínimo, 04 interfaces de rede 10 Gbps SFP+;
- 8.6.14. Deverá possuir, no mínimo, 08 interfaces de rede RJ-45 10/100/1000 Mbps, estando incluída uma interface para gerenciamento;
- 8.6.15. Deverá possuir, no mínimo, duas interfaces dedicadas para alta disponibilidade. Caso não possua, deverá possuir mais, no mínimo, duas interfaces RJ-45 10/100/1000 Mbps que possam ser utilizadas para esse fim (além das interfaces citadas no item 8.3.14, ou seja, um total de, no mínimo, 10 (dez) interfaces RJ-45 10/100/1000 Mbps;
- 8.6.16. Deverá possuir, no mínimo, 1 (uma) interface do tipo console ou similar;
- 8.6.17. Deverá ser incluído 4 (quatro) módulos transceivers 10 GE SFP+;
- 8.6.18. Deverá ser do tipo bidirecional (transmissão e recepção utilizando apenas uma fibra óptica);
- 8.6.19. Deverá ser do tipo short range;
- 8.6.20. Os módulos transceivers devem ser compatíveis com switchs dos seguintes fabricantes: Cisco, HP, Huawei e Extreme;
- 8.6.21. Deverá suportar, no mínimo, 60 (sessenta) zonas de segurança;
- 8.6.22. Deverá estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) clientes de VPN SSL simultâneos;
- 8.6.23. Deverá estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) túneis de VPN IPSEC simultâneos;
- 8.6.24. Deverá suportar, no mínimo, 1 (um) sistema virtual lógico (Contexto) no firewall Físico;
- 8.6.25. Os contextos virtuais deverão suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;
- 8.6.26. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale ou qualquer outra forma de lista de descontinuidade;
- 8.6.27. O item proposto deverá possuir pelo menos as seguintes funcionalidades:
- 8.6.28. Suportar sub-interfaces ethernet lógicas;
- 8.6.29. O firewall deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deverá estar

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
comunicável através de uma rota. Caso haja falha na comunicação o firewall  
deverá ter a capacidade de usar rota alternativa para estabelecer a comunicação;

8.6.30. Deverá suportar os seguintes tipos de NAT:

Nat dinâmico (Many-to-1);  
Nat dinâmico (Many-to-Many);  
Nat estático (1-to-1);  
NAT estático (Many-to-Many);  
Nat estático bidirecional 1-to-1;  
Tradução de porta (PAT);  
NAT de Origem;  
NAT de Destino;  
Suportar NAT de Origem e NAT de Destino simultaneamente;

8.6.31. O item proposto deverá possuir as seguintes funcionalidades:

Suporte a 4094 VLAN Tags 802.1q;  
Agregação de links 802.3ad e LACP;  
Policy based routing ou policy-based forwarding;  
DHCP Relay;  
DHCP Server;  
Suporte a criação de objetos de rede que possam ser utilizados como endereço  
IP de interfaces L3;

8.6.32. Deverá implementar balanceamento de link através de políticas por usuário e/ou  
grupos de usuários do LDAP/AD;

8.6.33. Deverá implementar balanceamento de link através de políticas por aplicação e  
porta de destino;

8.6.34. Deverá implementar o protocolo Link Layer Discovery (LLDP), permitindo que  
o appliance e outros ativos da rede se comuniquem para identificação da  
topologia da rede em que estão conectados e a função dos mesmos facilitando o  
processo de troubleshooting. As informações aprendidas e armazenadas pelo  
appliance deverão ser acessíveis via SNMP;

8.6.35. Deverá os registros de logs para sistemas de monitoração externos,  
simultaneamente. Deverá haver a opção de enviar logs via protocolo TCP e SSL;

8.6.36. Deverá permitir configurar certificado caso necessário para autenticação no  
sistema de monitoração externo de logs;

8.6.37. Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall,  
incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

8.6.38. Deverá implementar Proteção contra anti-spoofing;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.39. Deverá permitir bloquear sessões TCP que usem variações do 3-way handshake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
- 8.6.40. Deverá permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
- 8.6.41. Deverá suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64 ou Dual stack IPv4/IPv6, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPsec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPsec, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNS), DNS Search List (DNSSL) e controle de aplicação;
- 8.6.42. Os dispositivos de proteção deverão ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade<sup>15</sup> e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 8.6.43. Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
- Em modo transparente;
- Em layer 3;
- 8.6.44. A configuração em alta disponibilidade deverá sincronizar:
- Sessões;
- Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
- Certificados decriptografados;
- Associações de Segurança das VPNs;
- Tabelas FIB;
- O HA (modo de Alta-Disponibilidade) deverá possibilitar monitoração de falha de link.
- 8.6.45. As funcionalidades de firewall, IDS/IPS, identificação de usuários, controle de aplicações, VPN IPsec e SSL, QOS, decriptografia SSL e SSH, DHCP server,

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.46. DHCP relay, NAT, suporte a VLAN e protocolos de roteamento dinâmico deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
- 8.6.47. Deverá suportar controles por zona de segurança.
- 8.6.48. Controles de políticas por porta e protocolo.
- 8.6.49. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
- 8.6.50. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- 8.6.51. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- 8.6.52. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
- 8.6.53. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- 8.6.54. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
- 8.6.55. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
- 8.6.56. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- 8.6.57. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2 , TLS 1.2 e 1.3;
- 8.6.58. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- 8.6.59. Controle de inspeção e de-criptografia de SSH por política;
- 8.6.60. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
- 8.6.61. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.62. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.
- 8.6.63. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 8.6.64. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 8.6.65. Suporte a objetos e regras IPV6.
- 8.6.66. Suporte a objetos e regras multicast.
- 8.6.67. Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- 8.6.68. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 8.6.69. Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.
- 8.6.70. Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação). O fluxo mínimo de análise de regras legadas deve trabalhar dentro de um período de no mínimo 30 dias, permitindo a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.
- 8.6.71. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
- 8.6.72. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
- 8.6.73. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 8.6.74. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail,

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

- 8.6.75. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
- 8.6.76. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
- 8.6.77. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.
- 8.6.78. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 8.6.79. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
- 8.6.80. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;
- 8.6.81. Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc;
- 8.6.82. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 8.6.83. Atualizar a base de assinaturas de aplicações automaticamente;
- 8.6.84. Reconhecer aplicações em IPv6;
- 8.6.85. Limitar a banda (download/upload) usada por aplicações (traffic shaping),

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
baseado no IP de origem, usuários e grupos do LDAP/AD;

- 8.6.86. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- 8.6.87. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 8.6.88. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
- 8.6.89. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- 8.6.90. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica do item proposto, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- 8.6.91. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:
- 8.6.92. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
- 8.6.93. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 8.6.94. Deve alertar o usuário quando uma aplicação for bloqueada;
- 8.6.95. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 8.6.96. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
- 8.6.97. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesma, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
- 8.6.98. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
- 8.6.99. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.100. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 8.6.101. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 8.6.102. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
- 8.6.103. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 8.6.104. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
- 8.6.105. Tecnologia utilizada na aplicações (Client-Server, Browser Based, Network Protocol, etc).
- 8.6.106. Nível de risco da aplicação.
- 8.6.107. Categoria e subcategoria de aplicações.
- 8.6.108. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.
- 8.6.109. Deve permitir a inserção de duplo fator de autenticação na política de segurança não limitando a VPN apenas no mínimo para certificados, One-Time-Password ou Token de Software.
- 8.6.110. Deve proteger as aplicações contra movimentos laterais através da implementação de múltiplos fatores de autenticação.
- 8.6.111. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.
- 8.6.112. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 8.6.113. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
- 8.6.114. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.115. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
- 8.6.116. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;
- 8.6.117. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 8.6.118. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;
- 8.6.119. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
- 8.6.120. Deve permitir o bloqueio de vulnerabilidades.
- 8.6.121. Deve permitir o bloqueio de exploits conhecidos.
- 8.6.122. Deve incluir proteção contra ataques de negação de serviços.
- 8.6.123. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;
- 8.6.124. Deverá possuir os seguintes mecanismos de inspeção de IPS:
- 8.6.125. Análise de padrões de estado de conexões;
- 8.6.126. Análise de decodificação de protocolo;
- 8.6.127. Análise para detecção de anomalias de protocolo;
- 8.6.128. Análise heurística;
- 8.6.129. IP Defragmentation;
- 8.6.130. Remontagem de pacotes de TCP;
- 8.6.131. Bloqueio de pacotes malformados.
- 8.6.132. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;
- 8.6.133. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.134. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 8.6.135. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
- 8.6.136. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 8.6.137. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 8.6.138. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 8.6.139. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 8.6.140. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 8.6.141. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;
- 8.6.142. Suportar bloqueio de arquivos por tipo;
- 8.6.143. Identificar e bloquear comunicação com botnets;
- 8.6.144. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
- 8.6.145. Deve suportar referência cruzada com CVE;
- 8.6.146. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
- 8.6.147. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 8.6.148. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;
- 8.6.149. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;
- 8.6.150. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.151. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 8.6.152. Os eventos devem identificar o país de onde partiu a ameaça;
- 8.6.153. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 8.6.154. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.
- 8.6.155. Rastreamento de vírus em pdf.
- 8.6.156. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
- 8.6.157. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 8.6.158. Deve Permitir a importação, criação e edição de regras SNORT.
- 8.6.159. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, o item ofertado deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
- 8.6.160. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
- 8.6.161. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 8.6.162. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;
- 8.6.163. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
- 8.6.164. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP e Windows 7;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.165. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
- 8.6.166. O item ofertado deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;
- 8.6.167. A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL do item proposto;
- 8.6.168. Para ameaças trafegadas em protocolo SMTP e POP3, o item proposto deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
- 8.6.169. O sistema de análise "In Cloud" 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 Antivírus 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);
- 8.6.170. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais antivírus existentes no mercado possuem assinaturas para bloquear o malware;
- 8.6.171. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
- 8.6.172. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
- 8.6.173. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
- 8.6.174. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.
- 8.6.175. Caso o item proposto seja fornecido em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;
- 8.6.176. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

fornecidas em sua totalidade, sem custos adicionais para a CONTRATANTE;

- 8.6.177. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 8.6.178. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;
- 8.6.179. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;
- 8.6.180. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
- 8.6.181. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus do item proposto;
- 8.6.182. O item proposto deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executem esta função.
- 8.6.183. Deve prevenir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.
- 8.6.184. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
- 8.6.185. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 8.6.186. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
- 8.6.187. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.
- 8.6.188. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
- 8.6.189. Possui pelo menos 60 categorias de URLs;
- 8.6.190. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
- 8.6.191. Deve possuir categoria específica para classificar domínios recém registrados

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
(com menos de 32 dias);

- 8.6.192. Do item proposto deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
- 8.6.193. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
- 8.6.194. Suporta a criação categorias de URLs customizadas;
- 8.6.195. Suporta a exclusão de URLs do bloqueio, por categoria;
- 8.6.196. Permite a customização de página de bloqueio;
- 8.6.197. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados no item proposto;
- 8.6.198. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL do item proposto;
- 8.6.199. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);
- 8.6.200. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
- 8.6.201. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;
- 8.6.202. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
- 8.6.203. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 8.6.204. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 8.6.205. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

- 8.6.206. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 8.6.207. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e NAC via syslog, para a identificação de endereços IP e usuários;
- 8.6.208. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 8.6.209. Suporte a autenticação Kerberos;
- 8.6.210. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
- 8.6.211. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 8.6.212. Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
- 8.6.213. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;
- 8.6.214. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;
- 8.6.215. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 8.6.216. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.
- 8.6.217. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que o item proposto, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.218. Suportar a criação de políticas de QoS por:
- 8.6.219. Endereço de origem
- 8.6.220. Endereço de destino
- 8.6.221. Por usuário e grupo do LDAP/AD.
- 8.6.222. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 8.6.223. Por porta;
- 8.6.224. O QoS deve possibilitar a definição de classes por:
- 8.6.225. Banda Garantida
- 8.6.226. Banda Máxima
- 8.6.227. Fila de Prioridade.
- 8.6.228. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
- 8.6.229. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 8.6.230. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);
- 8.6.231. Disponibilizar estatísticas RealTime para classes de QoS.
- 8.6.232. Deve suportar QOS (traffic-shapping), em interface agregadas;
- 8.6.233. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.
- 8.6.234. Permite a criação de filtros para arquivos e dados pré-definidos;
- 8.6.235. Os arquivos devem ser identificados por extensão e assinaturas;
- 8.6.236. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
- 8.6.237. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.6.238. Permitir identificar e opcionalmente prevenir a transferência de informações

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

8.6.239. Permitir listar o número de aplicações suportadas para controle de dados;

8.6.240. Permitir listar o número de tipos de arquivos suportados para controle de dados;

8.6.241. Geo-localização

8.6.242. Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado País/Países sejam bloqueados.

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

8.6.244. Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;

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

8.6.246. Suportar VPN Site-to-Site e Cliente-To-Site;

8.6.247. Suportar IPSec VPN;

8.6.248. Suportar SSL VPN;

8.6.249. A VPN IPSEc deve suportar:

8.6.250. 3DES;

8.6.251. Autenticação MD5 e SHA-1;

8.6.252. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

8.6.253. Algoritmo Internet Key Exchange (IKEv1 e v2);

8.6.254. AES 128, 192 e 256 (Advanced Encryption Standard)

8.6.255. Autenticação via certificado IKE PKI.

8.6.256. Deve possuir interoperabilidade com os seguintes fabricantes:

8.6.257. Cisco;

8.6.258. Checkpoint;

8.6.259. Juniper;

8.6.260. Palo Alto Networks;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.261. Fortinet;
- 8.6.262. Sonic Wall;
- 8.6.263. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica do item proposto, facilitando o processo de troubleshooting;
- 8.6.264. A VPN SSL deve suportar:
  - 8.6.265. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
  - 8.6.266. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
  - 8.6.267. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
  - 8.6.268. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
  - 8.6.269. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
  - 8.6.270. Atribuição de DNS nos clientes remotos de VPN;
  - 8.6.271. Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
  - 8.6.272. A proposta de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
  - 8.6.273. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
  - 8.6.274. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
  - 8.6.275. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
  - 8.6.276. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.277. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 8.6.278. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
- 8.6.279. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
- 8.6.280. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- 8.6.281. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
- 8.6.282. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma proposta de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
- 8.6.283. Suporta leitura e verificação de CRL (certificate revocation list);
- 8.6.284. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 8.6.285. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- 8.6.286. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
- 8.6.287. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
- 8.6.288. Antes do usuário autenticar na estação;
- 8.6.289. Após autenticação do usuário na estação;
- 8.6.290. Sob demanda do usuário;
- 8.6.291. Deve Manter uma conexão segura com o portal durante a sessão.
- 8.6.292. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSX e Chrome OS;
- 8.6.293. O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID) e sistemas operacionais Linux;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.294. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;
- 8.6.295. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;
- 8.6.296. O item proposto deve permitir a quarentena automática e manual de dispositivos caso encontre algum comprometimento malicioso no tráfego inspecionado. Caso não possua essa funcionalidade será permitido integrações com outras como NAC (Network Access Control) ou SOAR (Security Orchestration Automation and Response).
- 8.6.297. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;
- 8.6.298. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
- 8.6.299. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
- 8.6.300. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;
- 8.6.301. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
- 8.6.302. O gerenciamento do item proposto deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 8.6.303. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente no próprio item proposto ou importado de fonte externa;
- 8.6.304. Caso haja a necessidade de instalação de cliente para administração do item proposto, o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
- 8.6.305. O gerenciamento deve permitir/possuir:
- 8.6.306. Criação e administração de políticas de firewall e controle de aplicação;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.307. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 8.6.308. Criação e administração de políticas de Filtro de URL;
- 8.6.309. Monitoração de logs;
- 8.6.310. Ferramentas de investigação de logs;
- 8.6.311. Debugging;
- 8.6.312. Captura de pacotes.
- 8.6.313. Acesso concorrente de administradores;
- 8.6.314. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
- 8.6.315. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.
- 8.6.316. Deve possuir mecanismo busca global no item proposto onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;
- 8.6.317. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- 8.6.318. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
- 8.6.319. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
- 8.6.320. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
- 8.6.321. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- 8.6.322. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 8.6.323. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.324. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- 8.6.325. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
- 8.6.326. Criação de regras que fiquem ativas em horário definido;
- 8.6.327. Criação de regras com data de expiração;
- 8.6.328. Backup das configurações e rollback de configuração para a última configuração salva;
- 8.6.329. Suportar Rollback de Sistema Operacional para a última versão local;
- 8.6.330. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
- 8.6.331. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
- 8.6.332. Validação de regras antes da aplicação;
- 8.6.333. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
- 8.6.334. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
- 8.6.335. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 8.6.336. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 8.6.337. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
- 8.6.338. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
- 8.6.339. Deve possibilitar a integração com outras de SIEM de mercado (third-party SIEM vendors)
- 8.6.340. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.341. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
- 8.6.342. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- 8.6.343. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
- 8.6.344. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;
- 8.6.345. O gerenciamento do item proposto deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- 8.6.346. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.
- 8.6.347. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;
- 8.6.348. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pelo item proposto;
- 8.6.349. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
- 8.6.350. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
- 8.6.351. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
- 8.6.352. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
- 8.6.353. Deve ser possível exportar os logs em CSV;
- 8.6.354. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
totalmente utilizada.

- 8.6.355. Rotação do log;
- 8.6.356. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados no item proposto, assim como no espaço em disco usado;
- 8.6.357. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
- 8.6.358. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
- 8.6.359. Situação do dispositivo e do cluster;
- 8.6.360. Principais aplicações;
- 8.6.361. Principais aplicações por risco;
- 8.6.362. Administradores autenticados na gerência da plataforma de segurança;
- 8.6.363. Número de sessões simultâneas;
- 8.6.364. Status das interfaces;
- 8.6.365. Uso de CPU;
- 8.6.366. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
- 8.6.367. Resumo gráfico de aplicações utilizadas;
- 8.6.368. Principais aplicações por utilização de largura de banda de entrada e saída;
- 8.6.369. Principais aplicações por taxa de transferência de bytes;
- 8.6.370. Principais hosts por número de ameaças identificadas;
- 8.6.371. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;
- 8.6.372. Deve permitir a criação de relatórios personalizados;
- 8.6.373. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.374. Gerar alertas automáticos via:
- 8.6.375. Email;
- 8.6.376. SNMP;
- 8.6.377. Syslog;
- 8.6.378. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com o item proposto possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.
- 8.6.379. O item proposto deverá identificar e categorizar novos dispositivos IoT sem a necessidade de realizar atividades intrusivas no ambiente de redes, tais como *port scans* e tentativas de acesso aos dispositivos a serem monitorados
- 8.6.380. A identificação e categorização dos dispositivos IoT deve ser realizada utilizando técnicas de Aprendizado de Máquina (Machine Learning), de forma a aumentar a acuracidade da identificação
- 8.6.381. O sistema de segurança IoT deve detectar e manter continuamente as informações de padrão de comportamento dos dispositivos
- 8.6.382. A identificação e categorização de novos dispositivos IoT que sejam implantados no ambiente monitorado pelo sistema de segurança IoT deverá ser realizada de forma automática, sem necessidade de nenhuma ação do operador ou administrador do item proposto.
- 8.6.383. O sistema de segurança IoT deve usar Aprendizado de Máquina (Machine Learning) para gerar automaticamente recomendações de políticas de segurança com base nos comportamentos de rede normais e aceitáveis dos dispositivos IoT de uma mesma categoria.
- 8.6.384. O sistema de segurança IoT deverá pelo menos identificar e categorizar dispositivos de TI tradicional (computadores, smartphones e dispositivos de rede) existentes no ambiente de redes monitorado
- 8.6.385. Deve permitir a visualização do comportamento de rede dos dispositivos IoT organizada por destinos de comunicação internos e externos
- 8.6.386. Deve ser possível criar conjuntos de políticas baseadas nos comportamentos de rede dos dispositivo IoT
- 8.6.387. O sistema de segurança IoT deve permitir a aplicação das recomendações de

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
políticas de segurança no NGFW, de forma a realizar o bloqueio do tráfego indesejado

- 8.6.388. Deve possuir mecanismo de identificação do dispositivo IoT baseado em atributos de Tipo, Fabricante e Modelo do dispositivo
- 8.6.389. Deve permitir utilizar os atributos de identificação do dispositivo como critério para a construção de políticas de segurança que realizem o bloqueio de tráfego indesejado
- 8.6.390. O sistema de segurança IoT deverá pelo menos identificar e categorizar dispositivos de TI tradicional (computadores, smartphones e dispositivos de rede) existentes no ambiente de redes monitorado
- 8.6.391. O sistema de segurança IoT deve identificar o tráfego de rede, as aplicações e a topologia da rede com as informações de conexões internas e externas para um dispositivo IoT
- 8.6.392. Deve permitir a visualização de um diagrama indicando as conexões de rede para um determinado dispositivo IoT, com a indicação de conexões que estão envolvidos em alertas de alta severidade
- 8.6.393. Deve utilizar técnicas de Aprendizado de Máquina (Machine Learning) para detectar vulnerabilidades nos dispositivos IoT e identificar seu nível de risco
- 8.6.394. As informações de vulnerabilidades devem conter, pelo menos, a severidade da vulnerabilidade, sua pontuação CVSS (Common Vulnerability Scoring System), seu nome ou código CVE (Common Vulnerabilities and Exposures) e se é uma vulnerabilidade confirmada ou potencial para os dispositivos
- 8.6.395. O sistema de segurança IoT deve mostrar as informações sumarizadas sobre uma vulnerabilidade encontrada, bem como seu impacto e as ações recomendadas para sua remediação
- 8.6.396. O sistema de segurança IoT deve usar técnicas de aprendizado de máquina de forma a identificar o comportamento normal de um dispositivo IoT e, ao detectar um comportamento anormal, gerar um alerta de segurança na console do item proposto;
- 8.6.397. O sistema de segurança IoT deve detectar a existência de ameaças de segurança do tráfego de um dispositivo IoT e gerar os respectivos alertas de segurança
- 8.6.398. Os detalhes de um alerta de segurança devem conter, pelo menos, as informações sobre o dispositivo IoT afetado, os protocolos de rede utilizados na conexão, seu impacto e as recomendações para remediação
- 8.6.399. Deve disponibilizar um dashboard de inventário de dispositivos IoT e também de TI tradicional que estejam em uso no ambiente de redes monitorado pelo item proposto, identificando os dispositivos monitorados e suas respectivas categorias.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.400. O item proposto para PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL deverá ser fornecida com software de gestão centralizada e armazenamento de logs com suporte e garantia de 03 anos, com as seguintes características:
- 8.6.401. Poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deverá ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deverá ser compatível com o hypervisor KVM;
- 8.6.402. Os softwares de gestão centralizada e armazenamento de logs poderão ser entregues em appliances separados, caso não seja possível entregar em um mesmo appliance;
- 8.6.403. O software deverá ser fornecido em sua versão mais atualizada;
- 8.6.404. Deverá possuir gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
- 8.6.405. O gerenciamento do item proposto deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
- 8.6.406. O Software de Gestão Centralizada deverá ser homologado e totalmente compatível com o item de PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL” especificado neste Termo de Referência para permitir o gerenciamento dos equipamentos e o armazenamento de logs gerados pelos mesmos;
- 8.6.407. Deverá permitir o armazenamento de logs sem limite de tempo para retenção e, em caso de esgotamento do espaço em disco disponibilizado para armazenamento dos logs, deverá ser realizado o log-rotation, conservando os dados mais recentes e excluindo os dados mais antigos;
- 8.6.408. Deverá permitir o armazenamento de logs sem limite de tempo e permitir alocar um no mínimo 20 TB;
- 8.6.409. Deverá permitir armazenar no mínimo 1,6 TB de logs por mês;
- 8.6.410. Deverá permitir armazenar no mínimo 50 GB de logs por dia;
- 8.6.411. Deverá permitir a exportação dos logs para outros sistemas;
- 8.6.412. Deverá permitir controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;
- 8.6.413. Deverá permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.6.414. Deverá permitir organizar os dispositivos administrados em grupos: os sistemas virtuais deverão ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
- 8.6.415. Deverá permitir implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
- 8.6.416. Deverá permitir a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
- 8.6.417. Deverá permitir a criação de objetos e políticas compartilhadas;
- 8.6.418. Deverá consolidar logs e relatórios de todos os dispositivos administrados;
- 8.6.419. Deverá permitir exportar backup de configuração automaticamente via agendamento;
- 8.6.420. Deverá permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;
- 8.6.421. Deverá exibir os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado.

**8.7. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DO ITEM DE PROTEÇÃO DE REDE COM CARACTERÍSTICAS DE NEXT GENERATION FIREWALL (NGFW) PARA SEGURANÇA DE INFORMAÇÃO PERIMETRAL**

- 8.7.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do item de proteção de rede com características NGFW, que compreendem, entre outros, os seguintes procedimentos:
- 8.7.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;
- 8.7.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
- 8.7.4. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;
- 8.7.5. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.7.6. Migração das regras de firewall existentes e aplicáveis do item de proteção de rede com características NGFW ofertado, considerando a adequação às políticas de aplicações em camada 7;
- 8.7.7. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pelo do item de proteção de rede ofertado;
- 8.7.8. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Anti-vírus e Anti-malware de acordo com as exigências levantadas;
- 8.7.9. Toda configuração de sistema (políticas gerais, objetos, itens de administração) deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante do item de proteção de rede com características NGFW ofertado. O fabricante do item ofertado deverá disponibilizar ferramenta gratuita (ou incluir nos custos de serviço) para acompanhamento da evolução da parametrização de proteção dos firewalls a fim de garantir a melhor eficiência durante o período de vigência das licenças;
- 8.7.10. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;
- 8.7.11. Durante a implantação a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
- 8.7.12. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
- 8.7.13. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE.

**8.8. SERVIDOR DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS  
DEFINIDO POR SOFTWARE**

- 8.8.1. O servidor de processamento e armazenamento de dados definido por software deverá prover uma estrutura de alta disponibilidade em permitindo configuração de cluster para ambiente de virtualização composta de unidades computacionais ou servidores físicos ou appliances ou nós, cada qual com sua respectiva capacidade de processamento, armazenamento e comunicação de rede. Neste cenário, deverá ser capaz de:
  - 8.8.1.1. Permitir escalabilidade horizontal, isso é, a adição de novos chassis e novos servidores (nós) ao cluster através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao hipervisor,

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
além de crescer de forma linear o desempenho/performance do ambiente;

- 8.8.1.2. O procedimento para expansão do cluster deverá ocorrer na mesma interface com assistente que permita tratar as configurações de endereços de rede e garanta que as versões já empregadas no cluster existente sejam transferidas para os novos equipamentos.
- 8.8.1.3. Permitir adição de um nó por vez.
- 8.8.1.4. Permitir adição de nós que incrementem apenas o armazenamento do cluster de forma independente do processamento e memória.
- 8.8.1.5. Permitir adição de novos equipamentos com geração mais recente no mesmo cluster.
- 8.8.1.6. Permitir remover equipamento do cluster sem parada no ambiente.
- 8.8.1.7. Criar um cluster lógico, agregando todos os discos físicos dos servidores contidos neste conjunto, apresentando um único sistema de arquivos ao hipervisor.
- 8.8.1.8. O item ofertado deve possuir funcionalidade para expor camada de armazenamento para aplicações físicas (bare metal) através do protocolo iSCSI ou NFS ou SMB.
- 8.8.1.9. Deverá suportar pelo menos dois Hipervisores. O item ofertado deve oferecer capacidade de conversão de clusters e de cargas de trabalho de um hipervisor para outro a fim de permitir adequação de custos durante renovações de suporte das licenças fornecidas ou aquisição de novas tecnologias de virtualização, preservando o investimento realizado.
- 8.8.1.10. Deverão ser fornecidas licenças necessárias para utilização de técnicas de otimização de armazenamento, como por exemplo, compressão e deduplicação.
- 8.8.1.11. Deverá garantir replicação síncrona de todos os dados gravados localmente para outros servidores que compõem o cluster para redundância dos dados, cada qual com seu respectivo sistema de armazenamento local com garantia de que a promoção e a demissão dos dados ocorram simultaneamente nos servidores do cluster.
- 8.8.1.12. A falha ou remoção de um disco não deve interromper o funcionamento de outros discos no mesmo equipamento. Caso o item proposto não atenda este requisito, deverá ser dimensionado prevendo tolerância a falha simultânea de dois equipamentos no mesmo cluster.
- 8.8.1.13. Todos os nós do cluster devem participar das operações de reconstrução de disco (rebuild), deixando-os mais eficientes à medida que o cluster cresce em número de nós. Caso o item proposto não atenda a este requisito, deverá ser ofertado com discos de até 3TB (três terabytes) a fim de minimizar o

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
impacto e o tempo de reconstrução.

- 8.8.2. A CONTRATADA deverá fornecer o licenciamento, suporte e subscrição, durante a vigência da garantia do item proposto, para o hipervisor nativo do proposto, com a respectiva gerenciamento centralizado, ambos em sua edição mais completa, de modo a permitir o uso de todas as suas funcionalidades para configuração e gerenciamento de um ambiente altamente disponível, sendo minimamente capaz de:
- 8.8.2.1. Permitir operações de live migration (migração da máquina virtual para outro host com a máquina virtual em operação);
  - 8.8.2.2. Disponibilizar gerenciador de imagens através de um repositório centralizado e permitir o uso de discos ou imagens nos formatos qcow, qcow2, vmdk, VHD, VHDx, raw, ISO para que seja possível a utilização destes discos e imagens com as máquinas virtuais do cluster;
  - 8.8.2.3. O item proposto deve ser capaz de distribuir os servidores virtuais entre os nós do cluster de modo que ocorra distribuição da carga.
- 8.8.3. O hipervisor deverá possuir um planejador (scheduler) com acesso a telemetria do host para tomar decisões de posicionamento das máquinas virtuais:
- 8.8.3.1. Posicionamento inicial: a melhor posição em um cluster para inicialização da máquina virtual ou carga de trabalho;
  - 8.8.3.2. Otimização de tempo de execução: movimento de cargas de trabalho com base em métricas durante tempo de execução.
- 8.8.4. O posicionamento das VMs deverá seguir pelo menos os seguintes fatores:
- 8.8.4.1. Computação (CPU/MEM)
  - 8.8.4.2. Utilização da CPU
  - 8.8.4.3. Utilização de memória
  - 8.8.4.4. Contenção de recursos
  - 8.8.4.5. Limiars e/ou marcas d'água para métricas de computação
  - 8.8.4.6. Desempenho de armazenamento
  - 8.8.4.7. Utilização do processo de gestão das operações de I/O
  - 8.8.4.8. Propriedade do disco virtual
  - 8.8.4.9. Localização dos volumes
  - 8.8.4.10. Regras de afinidade e anti-afinidade
  - 8.8.4.11. Políticas definidas pelo usuário para o local (host) onde será executada a VM
  - 8.8.4.12. Agrupamento de VMs
  - 8.8.4.13. Separação de VMs
- 8.8.5. Com intuito de simplificar as configurações de rede, deverá dispor de switch virtual distribuído baseado em, ou compatível com, Open Virtual Switch (OVS), de modo que a gestão seja centralizada e todas as configurações sejam igualmente

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
aplicadas e mantidas entre todos os hosts do cluster.

- 8.8.6. Para a rede virtual deverá permitir IP address management (IPAM) para a configuração de pools de endereços IP para atribuição às máquinas virtuais automaticamente sem a necessidade de um serviço de DHCP.
- 8.8.7. Deverá permitir a visualização de informações dos switches topo de rack na console Web de administração do cluster. Através do protocolo Link Layer Discovery Protocol (LLDP) ou Cisco Discovery Protocol (CDP), o item proposto deverá prover visualização gráfica das portas dos switches que estão conectadas às respectivas portas de redes das unidades computacionais. Adicionalmente, deverá ser possível a configuração dos protocolos SNMP v3 ou SNMP v2c nos switches topo de rack, para visualizar na mesma interface gráfica de gestão do cluster, as informações estatísticas das interfaces dos switches tais como:
  - 8.8.7.1. Número de pacotes unicast transmitidos e recebidos;
  - 8.8.7.2. Número de pacotes transmitidos e recebidos com um erro;
  - 8.8.7.3. Número de pacotes transmitidos e recebidos que foram descartados;
- 8.8.8. Permitir operações de alta disponibilidade automatizada, onde em caso de falha de um nó, as máquinas virtuais que dependam desse recurso, sejam automaticamente iniciadas em outro nó.
- 8.8.9. Ter uma ferramenta de planejamento de capacidade disponível, de forma a permitir a análise dos recursos e indicar máquinas virtuais subdimensionadas, superdimensionadas e inativas, para que seja possível identificação e remediação/otimização através da própria interface de gerenciamento centralizado. A ferramenta de planejamento de capacidade deve permitir simulações de provisionamento de novas aplicações com recomendações de otimização e eventuais capacidades ou equipamentos a serem adicionados ao cluster para que seja possível suportar estas novas aplicações. As simulações poderão ser executadas em múltiplos clusters com seus respectivos Hipervisores.
- 8.8.10. Permitir o monitoramento e análise dos elementos de hardware, storage e máquinas virtuais do cluster de modo que a detecção de anomalias no ambiente possam gerar alertas que permitam ao gerenciamento disparar ações automatizadas que possibilitem adequação dos recursos computacionais das máquinas virtuais tais como aumento e redução de processamento e memória, reinicialização de máquinas virtuais, envio de notificações para usuários e sistemas de mensageria, realização de snapshots, chamadas via APIs do tipo REST sem necessidade de intervenção do administrador.
- 8.8.11. O item proposto deve possuir console de administração WEB sem necessidade de instalação de qualquer componente adicional para essa finalidade;
- 8.8.12. O gerenciamento WEB deve ser capaz de gerenciar qualquer hipervisor especificado neste termo de referência;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.8.13. A console WEB deve ser acessível por browsers que suportam a tecnologia HTML5.
- 8.8.14. A console WEB deve fornecer acesso à um Dashboard principal personalizável com informações da saúde do Sistema (cluster) tanto no site local como em sites remotos, sumário dos equipamentos e das Máquinas Virtuais, visão geral da utilização dos recursos computacionais do cluster (processamento, memória, armazenamento), bem como visualização de alertas e eventos, visualização das informações de desempenho do item proposto (utilização de banda do cluster, IOPS do cluster e latência do cluster).
- 8.8.15. Deve permitir, através de uma interface de gestão gráfica, a atualização do storage definido por software, Hipervisor, BIOS e firmwares dos dispositivos de todos os equipamentos do cluster de forma simples e automatizada, eliminando a intervenção manual do administrador e parada no ambiente;
- 8.8.16. Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional em execução na proposta de *hiperconvergência* deverá oferecer REST APIs;
- 8.8.17. O gerenciador do cluster deve enviar periodicamente informações e estatísticas, de maneira automática, para o suporte. Esta funcionalidade tem por objetivo aplicar análises avançadas para otimizar a implementação ou atuar proativamente na identificação de problemas. Deverá ser permitido desabilitar este recurso a qualquer momento através da interface WEB;
- 8.8.18. Deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente;
- 8.8.19. Ferramenta de gerenciamento deve oferecer funcionalidade de planejamento de capacidade para crescimento baseado na carga de trabalho projetada;
- 8.8.20. Deve permitir que os usuários e administradores personalizem a visualização dos painéis de gerenciamento;
- 8.8.21. Ferramenta de gerenciamento deve possuir funcionalidade de busca (search) que suporte busca contextualizada;
- 8.8.22. A Ferramenta deve possuir a funcionalidade de criação de um portal de autosserviço, para que os usuários da infraestrutura disponibilizada pelo item proposto conforme suas permissões, possam Criar, Deletar e Acessar a console de seus servidores virtuais, sem a necessidade da intervenção do administrador do mesmo;
- 8.8.23. O Portal de Autosserviço, deve ter a capacidade de definir permissões específicas para os usuários dependendo de sua função (Role Based Access Control – RBAC), definidas pelo usuário gestor do item proposto, ou um usuário gestor do portal de autosserviço;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.8.24. Deve suportar o envio de alertas críticos automaticamente para o fabricante;
- 8.8.25. Deve suportar envio de alertas e eventos via SNMP;
- 8.8.26. Após a falha ou indisponibilidade de um equipamento (N+1), o cluster com pelo menos três equipamentos, deverá dispor de pelo menos 150TiB (cento e cinquenta tebibytes – base 2) de capacidade efetiva de armazenamento. A licitante poderá considerar ganhos com compressão e deduplicação de até 1.4:1. Não será aceita proposta dimensionada com erasure-coding.
- 8.8.27. Deverá ser comprovado o desempenho para banco de dados em cenário totalmente randômico com 70% de leitura, utilizando blocos de 8K, de pelo menos 30.000 IOPS (trinta mil operações de entrada e saída por segundo) para o cluster. O desempenho de IOPS deverá ser comprovado com latência inferior a 2ms (dois milissegundos). A comprovação poderá ser apresentada através de ferramenta de dimensionamento original do fabricante ou testes realizados em laboratório. A CONTRATANTE se reserva ao direito de realizar teste de bancada com o número mínimo de equipamentos necessários para simulação e comprovação do desempenho proposto.
- 8.8.28. Todos os requisitos de capacidade líquida, desempenho e tolerância a falha são mínimos. A licitante poderá ofertar seus equipamentos com os tipos de dispositivos de armazenamento mais adequados ao cumprimento de todos os requisitos estabelecidos.
- 8.8.29. Dos 150TiB de capacidade de armazenamento, 20TiB serão destinados ao armazenamento de arquivos para usuários e aplicações (NFS e SMB) e 10TiB ao armazenamento de objetos compatível com protocolo S3.
- 8.8.30. Caso a proposta de hiper convergência ofertada não suporte nativamente o armazenamento de arquivos (NFS e SMB) e de objetos (S3), é facultado a LICITANTE o fornecimento de unidade externa dedicada ao armazenamento de dados não estruturados. Neste caso, deverão ser entregues as mesmas capacidades líquidas e utilizáveis mínimas para o armazenamento de arquivos e para o armazenamento de objetos. O suporte para ambas (HCI e storage para dados não estruturados) deverá ser realizado pelo mesmo fabricante;
- 8.8.31. Em qualquer modelo de oferta, a deverá atender aos seguintes requisitos para armazenamento de arquivos:
- 8.8.31.1. Compartilhamento através de protocolos NFSv3 e NFSv4 e SMBv2 e SMBv3. Deverá estar devidamente dimensionada para suportar o número de 1.500 (um mil e quinhentos) usuários conectados de forma simultânea;
- 8.8.32. Deverá possuir arquitetura na modalidade "scale-out", ou seja, ser possível adicionar nós ou máquinas virtuais de acordo com a necessidade de performance, números de usuários conectados de forma simultânea ou escalabilidade de volumetria;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.8.33. Deverá suportar escalabilidade para pelo menos 5 (cinco) petabytes de volumetria útil;
- 8.8.34. Deverá ser composta de no mínimo 3 nós ou máquinas virtuais, e possuir sistema de Alta Disponibilidade Nativa para realizar o "fail-over" automático dos serviços para um nó ou máquina virtual remanescente em caso de falha;
- 8.8.35. Deverá possuir um assistente no próprio item ofertado para recomendações de "scale in", adição de recursos de CPU e/ou memória nos nós ou máquinas virtuais existentes ou "scale out", adição de novos nós ou máquinas virtuais com balanceamento de recursos baseado no nível de sua utilização;
- 8.8.36. Deverá suportar as seguintes funcionalidades para compartilhamento de arquivos via Protocolo SMB:
  - 8.8.37. Autenticação via Active Directory;
  - 8.8.38. Filtro de pasta e arquivos para listar apenas aqueles que o usuário possui permissão via Access-based enumeration (ABE);
  - 8.8.39. Habilitar assinatura digital para cada pacote enviado através da rede para assegurar a autenticidade e prevenir adulteração (SMB Signing);
  - 8.8.40. Habilitar encriptação em nível de pasta (SMB Encryption);
  - 8.8.41. Deverá suportar a organização de pastas compartilhadas entre diferentes servidores em um mesmo local ou geograficamente distantes através de um único "Single namespace", inserindo um diretório hierárquico unificado de modo a simplificar a integração com servidores de processamento e armazenamento de dados definido por software existentes ou futuros através do protocolo DFS-N (DFS Namespaces);
  - 8.8.42. Deverá suportar autenticação via "Active Directory", "LDAP" e acesso não gerenciado a compartilhamento via NFSv4 e autenticação via LDAP e acesso não gerenciado via protocolo NFSv3;
  - 8.8.43. Deverá suportar acesso multiprotocolo a uma ou mais pastas, ou seja, ser capaz de prover acesso tanto via SMB quanto via NFS a um mesmo compartilhamento utilizando de protocolos como Windos ACLs (Access Control Lists) e Unix mode bits;
  - 8.8.44. Deverá suportar a configuração de acesso a Home Share por nível de diretório (User Home Shares);
  - 8.8.45. Deverá suportar a otimização de um determinado compartilhamento de acordo com a natureza de tamanho do bloco, sendo possível personalizar entre:
  - 8.8.46. Padrão: 64KB por bloco;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.8.47. Randômico: 16KB por bloco;
- 8.8.48. Sequencial: 1MB por bloco;
- 8.8.49. O servidor de processamento e armazenamento de dados definido por software deverá possuir um painel de visualização de utilização que especifique as seguintes métricas em um intervalo mínimo de 7 dias:
- 8.8.50. Número de arquivos existentes;
- 8.8.51. Capacidade Utilizada;
- 8.8.52. Número de conexões abertas;
- 8.8.53. Espaço consumido por compartilhamento;
- 8.8.54. Deverá possuir um painel de visualização de performance que especifique as seguintes métricas em um intervalo mínimo de 7 dias:
- 8.8.55. Latência;
- 8.8.56. Banda (MB/s);
- 8.8.57. IOPs (I/O por segundo)
- 8.8.58. Deverá suportar a aplicação de cotas para controle de consumo do sistema de arquivos de forma granular a modo de avisar quando o usuário atingir consumo limite (soft limit) ou bloquear a escrita de novos arquivos (Hard limit). A cota deve ser possível de ser aplicada nos seguintes elementos:
- 8.8.59. Por usuário;
- 8.8.60. Por grupo;
- 8.8.61. Nível da própria pasta no momento de sua criação (Directory Level Quotas)
- 8.8.62. Deverá suportar o bloqueio de gravação de arquivos baseado em sua extensão a nível de servidor ou pasta, para os protocolos SMB, NFS e compartilhamentos multiprotocolo;
- 8.8.63. Deverá suportar o envio de eventos de notificação em tempo real como, criação, deleção, leitura, escrita e mudança de permissão em qualquer arquivo armazenado no servidor de processamento e armazenamento de dados definido por software a fim de retenção e auditoria através de opções como "syslog servers";
- 8.8.64. Deverá ser fornecido nativamente ou através de integração com software de terceiros, item proposto capaz de capturar os eventos de notificação e seja capaz de prover de forma simplificada um dashboard de auditoria que forneça no mínimo as seguintes informações:

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.8.64.1. Tendência de capacidade, com foco no que foi consumido e como foi na linha do tempo;
- 8.8.64.2. Idade dos arquivos, demonstrando cálculo de quando o arquivo foi alterado pela última vez e a porcentagem dos dados baseado no intervalo de variação de sua idade;
- 8.8.64.3. Detecção de anomalias, demonstrando todas as operações que excedem uma determinada política pré-determinada, como a deleção de múltiplos arquivos em um intervalo menor do que 1 (uma) hora;
- 8.8.64.4. Distribuição por tamanho e tipo de arquivo;
- 8.8.64.5. Ranking dos usuários mais ativos no sistema de armazenamento;
- 8.8.64.6. Ranking dos arquivos mais acessados no sistema de armazenamento;
- 8.8.64.7. Lista das operações mais frequentes (criação, escrita, leitura, deleção e alteração de permissionamento) seja pela média, tendência ou pico da operação;"
- 8.8.65. A auditoria deverá ser capaz de analisar e reter para consulta um tempo mínimo de 12 (doze) meses de dados capturados;
- 8.8.66. Deverá suportar a integração de software de anti-vírus de terceiros através do protocolo ICAP (Internet Content Adaptation Protocol) para compartilhamento via SMB e permitir a varredura de arquivos em tempo real quando o arquivo é aberto, fechado ou modificado.
- 8.8.67. A interface de gerenciamento de armazenamento do item proposto deverá mostrar o estado do arquivo após varredura de arquivos, tal como modo de quarentena, além dos eventos ocorridos com os mesmos (limpo, quarentena, deletado);
- 8.8.68. A interface de gerenciamento de armazenamento do item proposto deverá mostrar a lista de arquivos escaneados, as ameaças detectadas e os arquivos colocados em modo quarentena;
- 8.8.69. A interface de gerenciamento de armazenamento do item proposto deverá realizar ações voltadas aos arquivos, tais como:
  - 8.8.70. Rescan;
  - 8.8.71. Mover os arquivos para fora da Quarentena;
  - 8.8.72. Deletar arquivos na quarentena de forma permanente.
  - 8.8.73. Deverá suportar a criação de domínios de proteção de forma automatizada a fim de proteger com cópias locais e remotas a interface de gerenciamento de armazenamento do item proposto, através de agendamentos periódicos de snapshots (horas, dias, semanas e meses)
  - 8.8.74. Deverá suportar a possibilidade de recuperação a nível de arquivo pelo próprio usuário final (self service restore) baseado no agendamento de cópias locais

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

(snapshots) previamente estabelecidos. Para o protocolo SMB a recuperação deverá ser realizada pela propriedade de Versões Prévias da pasta destino. Para o protocolo NFS, através da listagem do subdiretório escondido (snapshot)

- 8.8.75. Deverá suportar a replicação remota habilitando a recuperação de desastres com intervalo mínimo de um minuto entre cópias para um segundo sistema de armazenamento ou cluster;
- 8.8.76. Referente ao Serviço de Armazenamento de Objetos, deverá ser configurado de maneira altamente disponível e distribuído, projetado com uma interface de API REST compatível com o Amazon Web Services Simple Storage Service (AWS S3) para lidar com dados não estruturados e gerados por máquina para fins de armazenamento para backup, armazenamento e retenção de longo prazo e desenvolvimento de aplicativos nativos para nuvem usando APIs padrão S3.
- 8.8.77. Também deverá possuir arquitetura na modalidade "scale-out", ou seja, ser possível adicionar nós, clusters ou máquinas virtuais de acordo com a necessidade de performance, números de requisições ou escalabilidade de volumetria;
- 8.8.78. O item proposto deverá estar devidamente dimensionado para suportar o número de 1.500 (mil e quinhentas) requisições por segundo;
- 8.8.79. O item proposto deverá possuir um assistente para criação de Object Stores capaz de dimensionar os recursos computacionais necessários com base no número de requisições por segundo e ainda permitir adequação destes recursos antes mesmo da criação do Object Store de acordo com a necessidade;
- 8.8.80. Permitir a criação de unidades organizacionais lógicas (buckets) para armazenamento dos objetos. Os objetos consistem em dados e metadados que descrevem os dados;
- 8.8.81. Deverá permitir a configuração de serviços de diretórios, compatível com Microsoft Active Directory e OpenLDAP, para adicionar facilmente pessoas que devem ter acesso a objetos;
- 8.8.82. Deverá permitir a geração e o controle de chaves de acesso para garantia de segurança;
- 8.8.83. O item proposto deverá permitir o compartilhamento dos "buckets" com os usuários que possuem as chaves de acesso, assim como, permitir a delegação de permissões como escrita e leitura de acordo com o nível de acesso
- 8.8.84. Deverá permitir a listagem dos buckets compartilhados, identificando quais usuários possuem acesso a cada um deles;
- 8.8.85. Deve ser possível gerenciar os buckets e seus respectivos objetos usando APIs REST compatíveis com o sistema de gerenciamento central do cluster ou S3 depois que um administrador autorizar os aplicativos e usuários a acessarem os buckets adequadamente;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.8.86. O item proposto deverá permitir o versionamento de múltiplas versões de um objeto dentro de um mesmo bucket. Opção deverá ser possível de ser habilitada na criação ou edição de um bucket existente;
- 8.8.87. O item proposto deverá permitir a criação de um conjunto de regras para definir ações do ciclo de vida de um objeto, como permitir que um objeto se apague automaticamente depois de um determinado número de dias, meses ou anos, assim como, apagar determinada versão de um objeto após um determinado período de tempo;
- 8.8.88. Deverá permitir a prevenção da deleção ou alteração de um objeto existente de acordo com um determinado período de retenção, utilizando de algoritmos de WORM (Write-Once-Rean-Many).
- 8.8.89. Deverá possuir painel de visualização de performance que demonstre a quantidade de requisições por segundo, banda utilizada (MB/s) e tempo de leitura de operação de leitura (GET);
- 8.8.90. Deverá suportar a atribuição de políticas de cotas de utilização notificando os respectivos usuários de acordo com nível de consumo de espaço ou número de buckets criados;
- 8.8.91. Deverá suportar o envio de eventos de notificação em tempo real como, criação, deleção, leitura, escrita e mudança de permissão em qualquer objeto armazenado a fim de retenção e auditoria através de opções como "syslog servers";
- 8.8.92. Todos os equipamentos e seus componentes deverão ser compatíveis.
- 8.8.93. Será aceita oferta de servidores do tipo appliances ou nós certificados desde que o item proposto contemple ferramenta de gestão e upgrades de versões dos firmwares, drivers e softwares relacionados de maneira centralizada, automatizada e com capacidade de orquestração para evacuação de máquinas virtuais e reinicialização de equipamentos sempre que necessário. O licenciamento dos softwares deverá permitir portabilidade para outros equipamentos e provedores de nuvem pública se necessário futuramente.
- 8.8.94. Todos os equipamentos deverão ser fornecidos com todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a, trilhos para montagem em rack, cabos de alimentação elétrica, além de todas as licenças de softwares necessárias para o funcionamento do item proposto conforme requisitos mínimos deste termo de referência.
- 8.8.95. Todos os recursos computacionais (processamento, memória e armazenamento) deverão ser úteis para as aplicações da CONTRATANTE, ou seja, deverão estar disponíveis para as aplicações após serem descontadas todas as perdas de armazenamento definida por software (SDS). Caso ocorra necessidade de manter uma infraestrutura separada para gerenciamento dos clusters, esta deverá ser fornecida pela CONTRATADA (hardware, softwares e serviços de instalação,

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
configuração e treinamento).

- 8.8.96. A licitante deverá então comprovar através de relatório extraído da ferramenta de dimensionamento ou manuais originais do respectivo fabricante, as perdas / overhead considerados na proposta. A CONTRATANTE também poderá exigir teste de bancada para comprovação dos requisitos editalícios.
- 8.8.97. Com o intuito de anular a exposição à vulnerabilidades conhecidas e ao mesmo tempo não haver perda de desempenho decorrente da correção não estrutural para estas vulnerabilidades, os processadores ofertados deverão ser da última geração disponível pelo fabricante do equipamento.
- 8.8.98. Objetivando atender aos requisitos de projetos de aprendizagem profunda (deep learning), os processadores deverão possuir instruções para redes neurais vetoriais (VNNI) compatíveis com AVX-512.
- 8.8.99. A configuração de memória dos equipamentos deverá ser constituída de maneira simétrica ocupando todos os canais de memória dos processadores com módulos idênticos em padrão e capacidade para garantia de melhor desempenho. Não serão aceitas configurações com módulos diferentes entre si.
- 8.8.100. Quanto a capacidade de armazenamento de dados, deverão ser calculadas e descontadas todas as perdas com formatação, configuração de RAID (quando aplicável) em nível para prover o melhor desempenho para o SDS, fator de replicação (dado original e uma réplica em equipamentos distintos no mesmo cluster e no mesmo site), alta-disponibilidade (HA), área de manobra (slack space) máxima e, também quando aplicável, grupos de discos em número máximo conforme estabelecido nos manuais do fabricante do item de armazenamento definida por software, para reduzir impacto durante operações de reconstrução e re-sincronização. Além disso, deverá considerar as perdas relativas à soma de verificação (checksum) para garantia de integridade dos dados e quaisquer outras perdas/overhead de armazenamento definida por software, inclusive perdas decorrentes do emprego de tecnologias para ganhos de eficiência como desduplicação e compressão.
- 8.8.101. A licitante poderá considerar ganhos com técnicas de desduplicação e compressão desde que estes ganhos sejam factíveis e não impossibilitem o atendimento aos demais requisitos deste Termo de Referência. Deverá estar licenciada para o uso destas funcionalidades. Caso o item proposto requeira evacuação dos dados e/ou reformatação dos discos para ativar ou desativar estas funcionalidades, a área de manobra (slack space) para esta evacuação deverá ser considerada com pelo menos 30% (trinta por cento) da capacidade do cluster, conforme recomendação expressa no manual do fabricante do sistema de armazenamento definida por software. Se o item proposto não for capaz de otimizar os dados no nível do cluster (global), a licitante deverá considerar 30% (trinta por cento) de capacidade de armazenamento útil adicional para o cluster a fim de compensar a ineficiência do sistema em manter cópias redundantes no cluster.
- 8.8.102. Para redução dos riscos de perda ou corrupção de dados em caso de falha de disco

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

durante processos de atualização de firmwares e softwares que requeiram reinicialização de equipamentos, a falha de um disco de cache ou de capacidade não deve impactar ou interromper o funcionamento de outros discos no item proposto. Caso não atenda este requisito, a capacidade de armazenamento útil do cluster deverá considerar a existência de três cópias dos dados (original e duas réplicas). Neste cenário a licitante também deverá considerar tempo de reposição de discos em no máximo 4h (quatro horas), a fim de reduzir o tempo e o impacto de reconstrução (rebuild) no cluster. O fabricante deverá garantir a troca de quaisquer discos mesmo quando as aplicações excederem seus limites de gravação (DWPD).

- 8.8.103. Para item proposto que dependam da configuração de RAID, as licitantes deverão considerar, no dimensionamento da capacidade útil, a quantidade de grupos de discos e o nível de RAID que garantam o melhor desempenho do item proposto ofertado conforme estabelecido nos manuais do respectivo fabricante do sistema de armazenamento definida por software.
- 8.8.104. Deverá possuir suporte com número de discagem gratuita e portal web para abertura de chamados;
- 8.8.105. Visará o emprego de configurações para um ambiente altamente disponível, com garantia e suporte técnico do fabricante durante 36 (trinta e seis) meses, na modalidade 24x7 com atendimento para chamados em até 1 (uma) hora e reposição de peças defeituosas até o próximo dia útil.
- 8.8.106. Cada equipamento deverá prover os seguintes recursos computacionais úteis para processamento das aplicações:
- 8.8.107. Processamento:
- 8.8.107.1. SPECrate2017\_int\_base 190 ou superior.
  - 8.8.107.2. Os processadores deverão operar a uma frequência mínima de 2.9GHz, inclusive na velocidade de comunicação com a memória.
  - 8.8.107.3. A definição de NUMA para execução das máquinas virtuais com o devido desempenho, cada CPU deverá prover pelo menos dezesseis núcleos de processamento.
- 8.8.108. Memória:
- 8.8.108.1. Pelo menos 730GB (setecentos e trinta gigabytes) de memória RAM ou superior.
- 8.8.109. Armazenamento:
- 8.8.109.1. A configuração de discos e agrupamentos necessária para atender a capacidade de 150TiB (cento e cinquenta tebibytes – base 2).

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

8.8.110. Comunicação:

8.8.110.1. Referente a capacidade de comunicação, cada equipamento que compõe deverá ser configurado com pelo menos 4 (quatro) portas de rede 10/25GbE com conectores SFP28 em placas idênticas entre si. Para cada porta de rede deverá ser fornecido um cabo de conexão direta tipo DAC ou Twinax de 3m (três metros) de comprimento para conexão com os switches MoR especificados neste edital.

**8.9. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SERVIDOR DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS DEFINIDO POR SOFTWARE**

- 8.9.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração de servidor de processamento e armazenamento de dados definido por software, que compreendem, entre outros, os seguintes procedimentos:
- 8.9.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;
- 8.9.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
- 8.9.4. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;
- 8.9.5. Durante a implantação a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados e será firmado termo de sigilo entre as partes;
- 8.9.6. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
- 8.9.7. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE
- 8.9.8. Devem ser realizados todos os ajustes de hardware e software necessários ao funcionamento dos equipamentos.
- 8.9.9. Todas as atualizações de firmware ou qualquer outro software componente, para a versão mais atualizada disponível ou a última compatível.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.9.10. Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.
- 8.9.11. Não compreende a instalação das aplicações, bem como a configuração das máquinas virtuais e migração de dados.

**8.10. SWITCH CORE CHASSIS MODULAR**

- 8.10.1. Deverá ser fornecido switch core modular com as seguintes características mínimas:
- 8.10.2. Deve possuir estrutura de chassi modular, para instalação em rack padrão EIA 19”, com no mínimo 08 (oito) slots para a inserção de módulos com interfaces, switching fabric e módulos de controle/supervisão;
- 8.10.3. Deve ser fornecido todos os acessórios necessários para a instalação do switch em rack 19”;
- 8.10.4. Deve ser fornecido com 2 (dois) módulos de gerenciamento;
- 8.10.5. Deve suportar no mínimo 4 Fontes de Alimentação operando em redundância e em modo load-sharing. Estas Fontes devem operar entre 110 a 220VAC. Devem também operar em 50/60Hz de frequência;
- 8.10.6. Deve ser fornecido com 4 (quatro) módulos de fonte;
- 8.10.7. Deve suportar módulos específicos de Controle, Switching-Fabric, estes devem ser configurados e estarem instalados de forma redundante, com pelo menos 02 (dois) módulos idênticos de cada, com entrada em operação automática em caso de falha de um deles;
- 8.10.8. Deve ser fornecido com 2 (dois) módulos Fabric;
- 8.10.9. Deve possuir todos os módulos, fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento;
- 8.10.10. Deve ser fornecido com no mínimo 9 (nove) módulos de ventilação;
- 8.10.11. Deve ser entregue com Sistema Operacional (IOS, Firmware, etc) na versão mais completa;
- 8.10.12. Deve suportar a instalação de no mínimo 48 portas 40/100 Gigabit Ethernet QSFP28;
- 8.10.13. Deve suportar a instalação de no mínimo 256 interfaces 1/10/25 Gigabit Ethernet SFP28+;
- 8.10.14. Deve suportar a instalação de no mínimo 256 interfaces 1/10 Gigabit Ethernet SFP+;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.10.15. Deve suportar a instalação de no mínimo 64 interfaces 40 Gigabit Ethernet QSFP+;
- 8.10.16. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
- 8.10.17. Deve possuir capacidade de comutação de, no mínimo, 19 Tbps;
- 8.10.18. Deve possuir capacidade de encaminhamento de, no mínimo, 7 BPPS;
- 8.10.19. Deve possuir interface de Console Serial ou USB;
- 8.10.20. Deve possuir uma porta para gerenciamento out-of-band com conector RJ-45;
- 8.10.21. Deve suportar permitir a agregação de links com LACP entre diferentes membros do switch virtual;
- 8.10.22. Deve implementar 802.3ad Agregação de Links incluindo entre portas de módulos distintos com mínimo de 128 grupos de 8 portas;
- 8.10.23. Deve permitir a agregação de links com LACP entre dois equipamentos autônomos (MC-LAG);
- 8.10.24. Deve possuir buffers de, no mínimo, 1,5 GB por módulo;
- 8.10.25. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 8.10.26. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
- 8.10.27. Deve implementar, no mínimo, 4.000(quatro mil) VLANs, conforme padrão IEEE 802.1q;
- 8.10.28. Deve implementar os seguintes padrões IEEE 802.1D, 802.1W, 802.1S, 802.1P
- 8.10.29. Deve implementar JUMBO FRAME (mínimo de 9k) em todas as interfaces Gigabit Ethernet;
- 8.10.30. Deve implementar LLDP (IEEE 802.1ab);
- 8.10.31. Deve implementar o padrão IEEE802.1AK;
- 8.10.32. Deve implementar MVRP;
- 8.10.33. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 8.10.34. Deve implementar MSTP (IEEE 802.1s) com suporte a 64 instâncias;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.10.35. Tabela de endereços MAC com capacidade para no mínimo 64.000 endereços MAC;
- 8.10.36. Deve possuir tabela de roteamento com 10.000 rotas IPv4 e 5.000 rotas IPv6;
- 8.10.37. Deve implementar roteamento estático;
- 8.10.38. Deve implementar roteamento OSPFv2 e OSPFv3;
- 8.10.39. Deve implementar roteamento OSPFv2 NSSA;
- 8.10.40. Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro;
- 8.10.41. Deve implementar roteamento OSPF com ECMP (Equal Cost Multi Path) de no mínimo, 8 grupos;
- 8.10.42. Deve implementar OSPF com “Graceful Restart”, que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado;
- 8.10.43. Deve implementar BGP;
- 8.10.44. Deve implementar BGP-4;
- 8.10.45. Deve implementar PRB (Policy Based Routing);
- 8.10.46. Deve implementar VRRP (Virtual Router Redundancy Protocol);
- 8.10.47. Deve implementar DHCP Client e DHCP Relay;
- 8.10.48. Deve suportar VRF ((Virtual Routing and Forwarding) até 32 VRFs Routing;
- 8.10.49. Deve implementar VRF Ipv4 e Ipv6;
- 8.10.50. Multicast:
- 8.10.51. Deve implementar PIM-SM;
- 8.10.52. Deve implementar IGMP nas versões v1 e v2 e Snooping;
- 8.10.53. Deve implementar MLD Snooping;
- 8.10.54. Deve implementar UDP Helper;
- 8.10.55. Deve implementar funcionalidade que proteja equipamento contra ARP Storm;
- 8.10.56. Deve implementar funcionalidade de proteção contra frames de BPDUs (spanning tree), no caso de recebimento de BPDUs, a porta deve ser colocada no estado de “down”;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.10.57. Deve possuir tecnologia que permite a separação do plano de dados (encaminhamento de pacotes) e do plano de controle;
- 8.10.58. Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas;
- 8.10.59. Deve implementar REST API;
- 8.10.60. Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado;
- 8.10.61. Deve implementar rate limiting para pacotes ICMP;
- 8.10.62. Deve implementar rate limiting para tráfego broadcast e multicast;
- 8.10.63. Deve suportar espelhamento de portas;
- 8.10.64. Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ
- 8.10.65. Deve suportar no mínimo, 8 (oito) filas de prioridade por porta;
- 8.10.66. Deve implementar ACL's do tipo Standard e Extended Ipv4 e Ipv6;
- 8.10.67. Deve suportar no mínimo 512 Access Control Entries (Egress)
- 8.10.68. Deve suportar no mínimo 1k Access Control Entries (Ingress)
- 8.10.69. Deve possuir RADIUS e TACACS+ para controle de gerenciamento do switch;
- 8.10.70. Deve suportar RADIUS/TACACS+ servers até 28 Server Groups
- 8.10.71. Deve suportar duas imagens de software na memória flash (IOS, Firmware);
- 8.10.72. Deve possuir capacidade de armazenar múltiplos arquivos de configuração;
- 8.10.73. Deve implementar sFlow (IPv4 e IPv6) ou similar;
- 8.10.74. Deve implementar TFTP, SFTP ou SCP para gerenciamento de software e configuração
- 8.10.75. Deve implementar SNMP v1, v2c e v3;
- 8.10.76. Deve possuir sincronização de horário (clock) do equipamento com servidor de tempo através do protocolo NTP ou SNTP
- 8.10.77. Deve suportar Self Signed Certificate Management
- 8.10.78. Deve suportar SSH v2

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.10.79. Deve suportar AAA (TACACS+ & RADIUS)
- 8.10.80. Deve implementar CLI com gerência por meio de linhas de comando;
- 8.10.81. Características físicas / ambientais:
- 8.10.82. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19";
- 8.10.83. Operar nas temperaturas de 0 a 40 °C;
- 8.10.84. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 8.10.85. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
- 8.10.86. Para fins de padronização, otimização e compatibilidade dos recursos e características, e perfeita interoperabilidade entre os equipamentos e software, todos os switches descritos neste termo de referência devem ser do mesmo fabricante;
- 8.10.87. O equipamento proposto deverá possuir garantia *onsite* do Fabricante de 3 (três) anos;
- 8.10.88. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento proposto, para fins de padronização, otimização de recursos, compatibilidade, gerência, garantia de fabricante, suporte e garantia de perfeita interoperabilidade entre os itens, deve ser do mesmo fabricante dos demais switches, do software de gerência e orquestração e do software de controle de acesso de rede descritos neste termo de referência.

**8.11. SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 1**

- 8.11.1. Características gerais do equipamento módulo para switch core chassis modular a ser fornecido:
- 8.11.2. Deve possuir pelo menos 6 (seis) portas QSFP28 40G/100G;
- 8.11.3. As portas devem ser Non-Blocking;
- 8.11.4. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do mesmo fabricante do switch core chassis modular descrito neste termo de referência.

**8.12. SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 2**

- 8.12.1. Características gerais do equipamento módulo para switch core chassis modular a ser fornecido:

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.12.2. Deve possuir pelo menos 8 (oito) portas QSFP+ 40G;
- 8.12.3. As portas devem ser Non-Blocking;
- 8.12.4. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do mesmo fabricante do switch core chassis modular descrito neste termo de referência.

**8.13. SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 3**

- 8.13.1. Características gerais do equipamento módulo para switch core chassis modular a ser fornecido:
- 8.13.2. Deve possuir pelo menos 32 (trinta e duas) portas SFP28 1G/10G/25G;
- 8.13.3. As portas devem ser Non-Blocking;
- 8.13.4. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do mesmo fabricante do switch core chassis modular descrito neste termo de referência.

**8.14. SWITCH CORE CHASSIS MODULAR - MÓDULO - TIPO 4**

- 8.14.1. Características gerais do equipamento módulo para switch core chassis modular a ser fornecido:
- 8.14.2. Deve possuir pelo menos 32 (trinta e duas) portas SFP+ 10G;
- 8.14.3. As portas devem ser Non-Blocking;
- 8.14.4. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do mesmo fabricante do switch core chassis modular descrito neste termo de referência.

**8.15. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH CORE**

- 8.15.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do switch core chassis modular, que compreendem, entre outros, os seguintes procedimentos:
- 8.15.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;
- 8.15.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
- 8.15.4. Conexão do equipamento switch core chassis modular na rede de comunicação de dados através de link de dados óptico ou metálico, designado para este fim;
- 8.15.5. Deverá prever a identificação física do equipamento switch core chassis modular;
- 8.15.6. Devem ser implantados os protocolos e serviços necessários e suficientes para

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

ativação e operação das funcionalidades do equipamento switch core chassis modular explorando suas características, dentro das melhores práticas de rede de computadores, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação;

- 8.15.7. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;
- 8.15.8. Durante a implantação a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
- 8.15.9. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
- 8.15.10. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE
- 8.15.11. Devem ser realizados todos os ajustes de hardware e software necessários ao funcionamento dos equipamentos.
- 8.15.12. Todas as atualizações de firmware ou qualquer outro software componente, para a versão mais atualizada disponível ou a última compatível.
- 8.15.13. Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.

**8.16. SWITCH DE AGREGAÇÃO**

- 8.16.1. Características gerais do equipamento switch de agregação a ser fornecido:
- 8.16.2. Deve possuir no mínimo 24 portas 1/10G SFP+;
- 8.16.3. Deve possuir 4 portas SFP56 adicionais com velocidade de 1/10/25/50G;
- 8.16.4. Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local;
- 8.16.5. Deve possuir uma interface de gerenciamento out of band;
- 8.16.6. Deve possuir memória RAM de no mínimo 8 Gbytes;
- 8.16.7. Deve possuir buffer de pacotes de no mínimo 8 MBytes;
- 8.16.8. Deve possuir capacidade de encaminhamento de no mínimo 660 Mpps;
- 8.16.9. Deve possuir capacidade de comutação de no mínimo 880 Gbps;
- 8.16.10. Deve possuir capacidade de empilhamento com até 10 elementos na pilha, sendo

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
gerenciados através de um único IP;

- 8.16.11. Deve ser possível realizar empilhamento em até 10Kms, utilizando transceivers de longa distância;
- 8.16.12. Deve possuir capacidade de empilhamento de 200Gbps;
- 8.16.13. Deve ser do tipo standalone, com altura máxima de 1RU e instalação em rack (19"). Deve acompanhar todos os componentes necessários para sua fixação no rack;
- 8.16.14. Deve possuir fonte de alimentação interna redundante e hot- swappable de 100/240VAC
- 8.16.15. Deve possuir fans redundantes e hot- swappable
- 8.16.16. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
- 8.16.17. Deve implementar VLAN 802.1Q;
- 8.16.18. Deve implementar 802.1V;
- 8.16.19. Deve implementar BPDU;
- 8.16.20. Deve possuir Jumbo Packets de no mínimo 9000 bytes;
- 8.16.21. Deve possuir Port Mirroring com no mínimo 4 grupos de espelhamento;
- 8.16.22. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 8.16.23. Deve implementar no mínimo 4094 VALN Ids;
- 8.16.24. Deve implementar MVRP (Multiple VLAN Registration Protocol);
- 8.16.25. Deve implementar LLDP (IEEE 802.1ab);
- 8.16.26. Deve implementar LLDP-MED;
- 8.16.27. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 8.16.28. Deve implementar MSTP (IEEE 802.1s);
- 8.16.29. Deve implementar MVRP
- 8.16.30. Deve implementar IGMP
- 8.16.31. Deve implementar túneis VxLAN (VTEP);
- 8.16.32. Deve implementar roteamento estático;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.16.33. Deve implementar OSPF;
- 8.16.34. Deve implementar OSPFv3;
- 8.16.35. Deve implementar BGP-4;
- 8.16.36. Deve implementar Policy-based Routing;
- 8.16.37. Deve implementar VRRP;
- 8.16.38. Deve implementar servidor DHCP;
- 8.16.39. Deve implementar DHCP snooping (IPv4 e IPv6);
- 8.16.40. Deve implementar DHCP relay;
- 8.16.41. Deve implementar VRF
- 8.16.42. Deve implementar BGP EVPN
- 8.16.43. Deve implementar PIM-SM;
- 8.16.44. Deve implementar PIM-DM;
- 8.16.45. Deve implementar MLD snooping;
- 8.16.46. Deve implementar IGMP v3;
- 8.16.47. Deve possuir interface REST API e scripting via Python
- 8.16.48. Deve possuir embarcado ferramenta customizável e programável para monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta on premise ou em cloud com que execute a mesma função e com todo licenciamento necessário pelo período mínimo de 36 meses.
- 8.16.49. Deve implementar controle de broadcast e multicast;
- 8.16.50. Deve implementar rate limiting para pacotes ICMP;
- 8.16.51. Deve implementar Strict priority (SP) queuing e Deficit Weighted Round Robin (DWRR)
- 8.16.52. Deve implementar priorização de trafego em tempo real;
- 8.16.53. Deve suportar IPSLA;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.16.54. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv;
- 8.16.55. Deve suporta pelo no mínimo oito filas de priorização de tráfego;
- 8.16.56. Deve suportar ACL para IPv4 e IPv6;
- 8.16.57. Deve implementar Acl com bas no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta;
- 8.16.58. Deve suportar controle de acesso baseado em perfis (Role Based Access Control)
- 8.16.59. Deve implementar 802.1x;
- 8.16.60. Deve implementar autenticação baseada em web;
- 8.16.61. Deve implementar autenticação baseada em endereço MAC;
- 8.16.62. Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas;
- 8.16.63. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 8.16.64. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 8.16.65. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam a rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
- 8.16.66. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, macOS e Linux.
- 8.16.67. Deve implementar NTP;
- 8.16.68. Deve suportar duas imagens de software na flash;
- 8.16.69. Deve suportar múltiplos arquivos de configuração na flash;
- 8.16.70. Deve suportar a auto-configuração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.16.71. Deve suportar detecção de falha e link entre switches;
- 8.16.72. Deve implementar sFlow;
- 8.16.73. Deve possuir interface web para configuração;
- 8.16.74. Deve implementar Syslog;
- 8.16.75. Deve implementar Secure SFTP (SFTP);
- 8.16.76. Deve implementar SNMP v1/v2/v3
- 8.16.77. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 8.16.78. Deve suportar o encaminhamento de tráfego para gateway do mesmo fabricante para inspeção e controle de acesso;
- 8.16.79. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 8.16.80. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
- 8.16.81. Para fins de padronização, otimização e compatibilidade dos recursos e características, e perfeita interoperabilidade entre os equipamentos e software, todos os switches descritos neste termo de referência devem ser do mesmo fabricante;
- 8.16.82. O equipamento proposto deverá possuir garantia *onsite* do Fabricante de 3 (três) anos;
- 8.16.83. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento proposto, para fins de padronização, otimização de recursos, compatibilidade, gerência, garantia de fabricante, suporte e garantia de perfeita interoperabilidade entre os itens, deve ser do mesmo fabricante dos demais switches, do software de gerência e orquestração e do software de controle de acesso de rede descritos neste termo de referência.

**8.17. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH DE AGREGAÇÃO**

- 8.17.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do switch de agregação, que compreendem, entre outros, os seguintes procedimentos:
- 8.17.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.17.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
- 8.17.4. Conexão do equipamento switch de agregação na rede de comunicação de dados através de link de dados óptico ou metálico, designado para este fim;
- 8.17.5. Deverá prever a identificação física do equipamento switch de agregação;
- 8.17.6. Devem ser implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades do equipamento switch de agregação explorando suas características, dentro das melhores práticas de rede de computadores, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação;
- 8.17.7. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;
- 8.17.8. Durante a implantação, a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
- 8.17.9. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
- 8.17.10. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE
- 8.17.11. Devem ser realizados todos os ajustes de hardware e software necessários ao funcionamento dos equipamentos.
- 8.17.12. Todas as atualizações de firmware ou qualquer outro software componente, para a versão mais atualizada disponível ou a última compatível.
- 8.17.13. Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.

**8.18. SWITCH DE ACESSO - TIPO 1**

- 8.18.1. Características gerais do equipamento switch de acesso tipo 1 a ser fornecido:
- 8.18.2. Deve possuir no mínimo 48 portas smart rate 100M/1G/2G/5G Ethernet Base T;
- 8.18.3. Deve possuir 4 portas SFP56 adicionais com velocidade de 1/10/25/50G;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.18.4. Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local;
- 8.18.5. Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af, IEEE 802.3at e IEEE 802.3bt;
- 8.18.6. Deve possuir capacidade de energização de 2880W;
- 8.18.7. Deve possuir uma interface de gerenciamento out of band;
- 8.18.8. Deve possuir memória RAM de no mínimo 8 Gbytes;
- 8.18.9. Deve possuir buffer de pacotes de no mínimo 8 Mbytes;
- 8.18.10. Deve possuir capacidade de encaminhamento de no mínimo 660 Mpps;
- 8.18.11. Deve possuir capacidade de comutação de no mínimo 880 Gbps;
- 8.18.12. Deve possuir capacidade de empilhamento com até 10 elementos na pilha, sendo gerenciados através de um único IP;
- 8.18.13. Deve ser possível realizar empilhamento em até 10Kms, utilizando transceivers de longa distância;
- 8.18.14. Deve possuir capacidade de empilhamento de 200Gbps;
- 8.18.15. O switch deve ser do tipo standalone, com altura máxima de 1RU e instalação em rack (19"). Deve acompanhar todos os componentes necessários para sua fixação no rack;
- 8.18.16. Deve suportar fonte de alimentação interna redundante e hot-swappable de 100/240VAC;
- 8.18.17. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
- 8.18.18. Deve implementar VLAN 802.1Q;
- 8.18.19. Deve implementar 802.1V;
- 8.18.20. Deve implementar BPDU;
- 8.18.21. Deve possuir Jumbo Packets de no mínimo 9000 bytes;
- 8.18.22. Deve implementar Port Mirroring com no mínimo 4 grupos de espelhamento;
- 8.18.23. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 8.18.24. Deve implementar 4094 VALN Ids;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.18.25. Deve implementar MVRP (Multiple VLAN Registration Protocol);
- 8.18.26. Deve implementar LLDP (IEEE 802.1ab);
- 8.18.27. Deve implementar LLDP-MED;
- 8.18.28. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 8.18.29. Deve implementar MSTP (IEEE 802.1s);
- 8.18.30. Deve implementar MVRP;
- 8.18.31. Deve implementar IGMP;
- 8.18.32. Deve implementar túneis VxLAN (VTEP);
- 8.18.33. Deve implementar roteamento estático;
- 8.18.34. Deve implementar OSPF;
- 8.18.35. Deve implementar OSPFv3;
- 8.18.36. Deve implementar BGP-4;
- 8.18.37. Deve implementar Policy-based Routing;
- 8.18.38. Deve implementar VRRP;
- 8.18.39. Deve implementar servidor DHCP;
- 8.18.40. Deve implementar DHCP snooping (IPv4 e IPv6);
- 8.18.41. Deve implementar DHCP relay;
- 8.18.42. Deve implementar VRF;
- 8.18.43. Deve implementar BGP EVPN;
- 8.18.44. Deve implementar PIM-SM;
- 8.18.45. Deve implementar PIM-DM;
- 8.18.46. Deve implementar MLD snooping;
- 8.18.47. Deve implementar IGMP v3;
- 8.18.48. Deve possuir interface REST API e scripting via Python
- 8.18.49. Deve possuir embarcado ferramenta customizável e programável para

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta on premise ou em cloud com que execute a mesma função e com todo licenciamento necessário pelo período mínimo de 36 meses;

- 8.18.50. Deve implementar controle de broadcast e multicast;
- 8.18.51. Deve implementar rate limiting para pacotes ICMP;
- 8.18.52. Deve implementar Strict priority (SP) queuing e Deficit Weighted Round Robin (DWRR)
- 8.18.53. Deve implementar priorização de tráfego em tempo real;
- 8.18.54. Deve suportar IPSLA;
- 8.18.55. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv;
- 8.18.56. Deve suporta pelo no mínimo oito filas de priorização de tráfego;
- 8.18.57. Deve suportar ACL para IPv4 e IPv6;
- 8.18.58. Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta;
- 8.18.59. Deve suportar controle de acesso baseado em perfis (Role Based Access Control);
- 8.18.60. Deve implementar 802.1x;
- 8.18.61. Deve implementar autenticação baseada em web;
- 8.18.62. Deve implementar autenticação baseada em endereço MAC;
- 8.18.63. Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas;
- 8.18.64. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 8.18.65. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 8.18.66. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam a rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.18.67. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, macOS e Linux.
- 8.18.68. Deve implementar NTP;
- 8.18.69. Deve suportar duas imagens de software na flash;
- 8.18.70. Deve suportar múltiplos arquivos de configuração na flash;
- 8.18.71. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 8.18.72. Deve suportar detecção de falha e link entre switches;
- 8.18.73. Deve implementar sFlow;
- 8.18.74. Deve possuir interface web para configuração;
- 8.18.75. Deve implementar Syslog;
- 8.18.76. Deve implementar Secure SFTP (SFTP);
- 8.18.77. Deve implementar SNMP v1/v2/v3
- 8.18.78. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 8.18.79. Deve suportar o encaminhamento de tráfego para gateway do mesmo fabricante para inspeção e controle de acesso;
- 8.18.80. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 8.18.81. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
- 8.18.82. Para fins de padronização, otimização e compatibilidade dos recursos e características, e perfeita interoperabilidade entre os equipamentos e software, todos os switches descritos neste termo de referência devem ser do mesmo fabricante;
- 8.18.83. O equipamento proposto deverá possuir garantia Onsite do Fabricante de 3 (três) anos;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

8.18.84. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, para fins de padronização, otimização de recursos, compatibilidade, gerência, garantia de fabricante, suporte e garantia de perfeita interoperabilidade entre os itens, deve ser do mesmo fabricante dos demais switches, do software de gerência e orquestração e do software de controle de acesso de rede descritos neste termo de referência.

**8.19. SWITCH DE ACESSO - TIPO 2**

- 8.19.1. Características gerais do equipamento switch de acesso tipo 2 a ser fornecido:
- 8.19.2. Deve possuir no mínimo 24 portas smart rate 100M/1G/2G/5G Ethernet Base T;
- 8.19.3. Deve possuir 4 portas SFP56 adicionais com velocidade de 1/10/25/50G;
- 8.19.4. Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local;
- 8.19.5. Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af, IEEE 802.3at e IEEE 802.3bt;
- 8.19.6. Deve possuir capacidade de energização de 1440W;
- 8.19.7. Deve possuir uma interface de gerenciamento out of band;
- 8.19.8. Deve possuir memória RAM de no mínimo 8 Gbytes;
- 8.19.9. Deve possuir buffer de pacotes de no mínimo 8 Mbytes;
- 8.19.10. Deve possuir capacidade de encaminhamento de no mínimo 660 Mpps;
- 8.19.11. Deve possuir capacidade de comutação de no mínimo 880 Gbps;
- 8.19.12. Deve possuir capacidade de empilhamento com até 10 elementos na pilha, sendo gerenciados através de um único IP;
- 8.19.13. Deve ser possível realizar empilhamento em até 10Kms, utilizando transceivers de longa distância;
- 8.19.14. Deve possuir capacidade de empilhamento de 200Gbps;
- 8.19.15. O switch deve ser do tipo standalone, com altura máxima de 1RU e instalação em rack (19"). Deve acompanhar todos os componentes necessários para sua fixação no rack;
- 8.19.16. Deve suportar fonte de alimentação interna redundante e hot- swappable de 100/240VAC;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.19.17. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
- 8.19.18. Funcionalidades de Camada 2:
- 8.19.19. Deve implementar VLAN 802.1Q;
- 8.19.20. Deve implementar 802.1V;
- 8.19.21. Deve implementar BPDU;
- 8.19.22. Deve possuir Jumbo Packets de no mínimo 9000 bytes;
- 8.19.23. Deve implementar Port Mirroring com no mínimo 4 grupos de espelhamento;
- 8.19.24. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
- 8.19.25. Deve implementar 4094 VALN Ids;
- 8.19.26. Deve implementar MVRP (Multiple VLAN Registration Protocol);
- 8.19.27. Deve implementar LLDP (IEEE 802.1ab);
- 8.19.28. Deve implementar LLDP-MED;
- 8.19.29. Deve implementar PVST+, RPVST+ ou protocolo compatível;
- 8.19.30. Deve implementar MSTP (IEEE 802.1s);
- 8.19.31. Deve implementar MVRP;
- 8.19.32. Deve implementar IGMP;
- 8.19.33. Deve implementar túneis VxLAN (VTEP);
- 8.19.34. Funcionalidades de Camada 3:
- 8.19.35. Deve implementar roteamento estático;
- 8.19.36. Deve implementar OSPF;
- 8.19.37. Deve implementar OSPFv3;
- 8.19.38. Deve implementar BGP-4;
- 8.19.39. Deve implementar Policy-based Routing;
- 8.19.40. Deve implementar VRRP;
- 8.19.41. Deve implementar servidor DHCP;
- 8.19.42. Deve implementar DHCP snooping (IPv4 e IPv6);

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.19.43. Deve implementar DHCP relay;
- 8.19.44. Deve implementar VRF;
- 8.19.45. Deve implementar BGP EVPN;
- 8.19.46. Multicast:
- 8.19.47. Deve implementar PIM-SM;
- 8.19.48. Deve implementar PIM-DM;
- 8.19.49. Deve implementar MLD snooping;
- 8.19.50. Deve implementar IGMP v3;
- 8.19.51. Software Defined Networking:
- 8.19.52. Deve possuir interface REST API e scripting via Python
- 8.19.53. Deve possuir embarcado ferramenta customizável e programável para monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta on premise ou em cloud com que execute a mesma função e com todo licenciamento necessário pelo período mínimo de 36 meses;
- 8.19.54. QoS e ACL:
- 8.19.55. Deve implementar controle de broadcast e multicast;
- 8.19.56. Deve implementar rate limiting para pacotes ICMP;
- 8.19.57. Deve implementar Strict priority (SP) queuing e Deficit Weighted Round Robin (DWRR)
- 8.19.58. Deve implementar priorização de trafego em tempo real;
- 8.19.59. Deve suportar IPSLA;
- 8.19.60. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv;
- 8.19.61. Deve suporta pelo no mínimo oito filas de priorização de tráfego;
- 8.19.62. Deve suportar ACL para IPv4 e IPv6;
- 8.19.63. Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.19.64. Deve suportar controle de acesso baseado em perfis (Role Based Access Control);
- 8.19.65. Deve implementar 802.1x;
- 8.19.66. Deve implementar autenticação baseada em web;
- 8.19.67. Deve implementar autenticação baseada em endereço MAC;
- 8.19.68. Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas;
- 8.19.69. Deve implementar TACACS+. Não serão aceitas soluções similares;
- 8.19.70. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
- 8.19.71. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam a rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
- 8.19.72. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, macOS e Linux.
- 8.19.73. Gerenciamento:
- 8.19.74. Deve implementar NTP;
- 8.19.75. Deve suportar duas imagens de software na flash;
- 8.19.76. Deve suportar múltiplos arquivos de configuração na flash;
- 8.19.77. Deve suportar a auto-configuração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
- 8.19.78. Deve suportar detecção de falha e link entre switches;
- 8.19.79. Deve implementar sFlow;
- 8.19.80. Deve possuir interface web para configuração;
- 8.19.81. Deve implementar Syslog;
- 8.19.82. Deve implementar Secure SFTP (SFTP);
- 8.19.83. Deve implementar SNMP v1/v2/v3

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.19.84. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;
- 8.19.85. Deve suportar o encaminhamento de tráfego para gateway do mesmo fabricante para inspeção e controle de acesso;
- 8.19.86. Licenciamento:
- 8.19.87. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
- 8.19.88. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
- 8.19.89. Para fins de padronização, otimização e compatibilidade dos recursos e características, e perfeita interoperabilidade entre os equipamentos e software, todos os switches descritos neste termo de referência devem ser do mesmo fabricante;
- 8.19.90. Garantia e Suporte:
- 8.19.91. O equipamento proposto deverá possuir garantia Onsite do Fabricante de 3 (três) anos;
- 8.19.92. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (para o horário comercial – horário oficial de Brasília);
- 8.19.93. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, para fins de padronização, otimização de recursos, compatibilidade, gerência, garantia de fabricante, suporte e garantia de perfeita interoperabilidade entre os itens, deve ser do mesmo fabricante dos demais switches, do software de gerência e orquestração e do software de controle de acesso de rede descritos neste termo de referência.

**8.20. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE SWITCH DE ACESSO TIPO 1 ou TIPO 2**

- 8.20.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do switch de acesso tipo 1 ou tipo 2, que compreendem, entre outros, os seguintes procedimentos:
- 8.20.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;
- 8.20.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares)

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);

- 8.20.4. Conexão do equipamento switch de acesso tipo 1 ou tipo 2 na rede de comunicação de dados através de link de dados óptico ou metálico, designado para este fim;
- 8.20.5. Deverá prever a identificação física do equipamento switch de acesso tipo 1 ou tipo 2;
- 8.20.6. Devem ser implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades do equipamento switch de acesso tipo 1 ou tipo 2 explorando suas características, dentro das melhores práticas de rede de computadores, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação;
- 8.20.7. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;
- 8.20.8. Durante a implantação, a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
- 8.20.9. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
- 8.20.10. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE
- 8.20.11. Devem ser realizados todos os ajustes de hardware e software necessários ao funcionamento dos equipamentos.
- 8.20.12. Todas as atualizações de firmware ou qualquer outro software componente, para a versão mais atualizada disponível ou a última compatível.
- 8.20.13. Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.

**8.21. TRANSCEIVER - TIPO 1**

- 8.21.1. Características gerais do equipamento a ser fornecido:
- 8.21.2. Transceiver SFP para conexão de fibras ópticas multimodo;
- 8.21.3. Deve ser compatível com o padrão SX para fibras ópticas de até 500m;
- 8.21.4. Deve possuir conector LC;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.21.5. Velocidade de 1 Gb;
- 8.21.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.21.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.22. TRANSCEIVER - TIPO 2**

- 8.22.1. Características gerais do equipamento a ser fornecido:
- 8.22.2. Transceiver SFP para conexão de fibras ópticas monomodo;
- 8.22.3. Deve ser compatível com o padrão LX para fibras ópticas de até 10Km;
- 8.22.4. Deve possuir conector LC;
- 8.22.5. Velocidade de 1 Gb;
- 8.22.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.22.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.23. TRANSCEIVER - TIPO 3**

- 8.23.1. Características gerais do equipamento a ser fornecido:
- 8.23.2. Transceiver SFP+ para conexão de fibras ópticas multimodo;
- 8.23.3. Deve ser compatível com o padrão SR para fibras ópticas de até 300m;
- 8.23.4. Deve possuir conector LC;
- 8.23.5. Velocidade de 10Gbps;
- 8.23.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.23.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção,

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

#### **8.24. TRANSCEIVER - TIPO 4**

- 8.24.1. Características gerais do equipamento a ser fornecido:
- 8.24.2. Transceiver SFP+ para conexão de fibras ópticas monomodo;
- 8.24.3. Deve ser compatível com o padrão LR para fibras ópticas de até 10Km;
- 8.24.4. Deve possuir conector LC;
- 8.24.5. Velocidade de 10Gbps;
- 8.24.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.24.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

#### **8.25. TRANSCEIVER - TIPO 5**

- 8.25.1. Características gerais do equipamento a ser fornecido:
- 8.25.2. Transceiver SFP28 para conexão de fibras ópticas multimodo;
- 8.25.3. Deve ser compatível com o padrão SR para fibras ópticas de até 100m;
- 8.25.4. Deve possuir conector LC;
- 8.25.5. Velocidade de 25Gbps;
- 8.25.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.25.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

#### **8.26. TRANSCEIVER - TIPO 6**

- 8.26.1. Características gerais do equipamento a ser fornecido:
- 8.26.2. Transceiver SFP28 para conexão de fibras ópticas monomodo;

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

- 8.26.3. Deve ser compatível com o padrão LR para fibras ópticas de até 10Km;
- 8.26.4. Deve possuir conector LC;
- 8.26.5. Velocidade de 25Gbps;
- 8.26.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.26.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.27. TRANSCEIVER - TIPO 7**

- 8.27.1. Características gerais do equipamento a ser fornecido:
- 8.27.2. Transceiver QSFP+ para conexão de fibras ópticas multimodo;
- 8.27.3. Deve ser compatível com o padrão BiDi para fibras ópticas de até 150m;
- 8.27.4. Deve possuir conector LC;
- 8.27.5. Velocidade de 40Gbps;
- 8.27.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.27.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.28. TRANSCEIVER - TIPO 8**

- 8.28.1. Características gerais do equipamento a ser fornecido:
- 8.28.2. Transceiver QSFP+ para conexão de fibras ópticas monomodo;
- 8.28.3. Deve ser compatível com o padrão LR4 para fibras ópticas de até 10Km;
- 8.28.4. Deve possuir conector LC;
- 8.28.5. Velocidade de 40Gbps;
- 8.28.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

- 8.28.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.29. TRANSCEIVER - TIPO 9**

- 8.29.1. Características gerais do equipamento a ser fornecido;
- 8.29.2. Transceiver QSFP28 para conexão de fibras ópticas monomodo;
- 8.29.3. Deve ser compatível com o padrão CWDM4 para fibras ópticas de até 2Km;
- 8.29.4. Deve possuir conector LC;
- 8.29.5. Velocidade de 100Gbps;
- 8.29.6. A garantia do transceiver deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.29.7. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.30. CABO PARA CONEXÃO DIRETA – TIPO 1**

- 8.30.1. Características gerais do equipamento a ser fornecido;
- 8.30.2. Deve possuir no mínimo 3 metros de comprimento;
- 8.30.3. Cabo de conexão do Tipo 10G SFP+ para SFP+;
- 8.30.4. A garantia do cabo deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.30.5. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.31. CABO PARA CONEXÃO DIRETA – TIPO 2**

- 8.31.1. Características gerais do equipamento a ser fornecido;
- 8.31.2. Deve possuir no mínimo 3 metros de comprimento;
- 8.31.3. Cabo de conexão do Tipo 25G SFP28 para SFP28;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.31.4. A garantia do cabo deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.31.5. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.32. CABO PARA CONEXÃO DIRETA – TIPO 3**

- 8.32.1. Características gerais do equipamento a ser fornecido:
- 8.32.2. Deve possuir no mínimo 7 metros de comprimento;
- 8.32.3. Cabo de conexão do Tipo 100G QSFP28 para QSFP28;
- 8.32.4. A garantia do cabo deve acompanhar a garantia dos switches descritos neste termo de referência;
- 8.32.5. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos switches descritos neste termo de referência.

**8.33. PONTO DE ACESSO SEM FIO - TIPO 1**

- 8.33.1. Características gerais do equipamento Ponto de Acesso sem fio Tipo 1 a ser fornecido:
- 8.33.2. Deve possuir 04 (quatro) antenas integradas ao equipamento, com padrão de irradiação omnidirecional, dual-band, com ganho de, pelo menos, 3.5 dBi em 2.4GHz e com ganho de, pelo menos, 5.0 dBi em 5GHz;
- 8.33.3. Deve suportar, utilizando a modulação OFDMA, a capacidade de transmitir simultaneamente clientes por canal, com as seguintes possibilidades:
- 8.33.4. Wi-Fi 6 operando com canais de 20MHz, até 09 (nove) clientes simultaneamente;
- 8.33.5. Wi-Fi 6 operando com canais de 40MHz, até 18 (dezoito) clientes simultaneamente;
- 8.33.6. Wi-Fi 6 operando com canais de 80MHz, até 37 (trinta e sete) clientes simultaneamente;
- 8.33.7. Wi-Fi 6 operando com canais de 160MHz, até 74 (setenta e quatro) clientes simultaneamente;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.33.8. Deve operar em 5GHz e 2.4GHz 4x4 MIMO;
- 8.33.9. Deve suportar operação em 5GHz com 04 (quatro) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 4.8Gbps;
- 8.33.10. Deve suportar operação em 5GHz com 02 (duas) vezes 01 (um) Spatial Stream Multi User (MU) MIMO;
- 8.33.11. Deve suportar operação em 2.4GHz com 02 (quatro) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 1,147Mbps;
- 8.33.12. Deve suportar operação em 2.4GHz com 02 (duas) vezes 01 (um) Spatial Streams Multi User (MU) MIMO;
- 8.33.13. Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas;
- 8.33.14. Possuir potência máxima de transmissão para frequências de 2.4GHz de no mínimo:
- 8.33.15. +24 dBm;
- 8.33.16. Possuir potência máxima de transmissão para frequências de 5GHz de no mínimo:
- 8.33.17. +24 dBm;
- 8.33.18. Capacidade de configurar a potência de transmissão em incrementos de 0.5 dBm;
- 8.33.19. Deve permitir funcionamento em modo gerenciado por controladora, para otimização de performance de rede, roaming, segurança, todos os Pontos de Acesso criam um túnel com todo tráfego centralizado para o gerenciamento;
- 8.33.20. Deve permitir funcionamento em modo auto gerenciado, sem a necessidade de uma controladora WLAN, onde o próprio Ponto de Acesso pode operar como um Controladora Virtual.
- 8.33.21. Deve permitir o gerenciamento através de plataforma nuvem (cloud).
- 8.33.22. Deve permitir o gerenciamento através de plataforma local (on-premise).
- 8.33.23. Para implementações em larga escala, o Ponto de Acesso deve configurar-se automaticamente ao ser conectado na rede, sendo provisionado através da ferramenta de gerenciamento;
- 8.33.24. Possuir LED's multicoloridos indicativos do estado de operação e da atividade do rádio;
- 8.33.25. Deve possuir 02 (duas) interfaces de rede SmartRate/Multigigabit (RJ-45) com velocidade de até 5Gbps com as seguintes características:
- 8.33.26. Auto-sensing link speed (100/1000/2500/5000BASE-T) e MDI/MDX;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.33.27. 2.5 Gbps e 5 Gbps speed conforme especificações de NBase-T e 802.3bz;
- 8.33.28. PoE-PD: 48Vdc (nominal) 802.3af/802.3at/802.3bt (classe ou superior);
- 8.33.29. 802.3az Energy Efficient Ethernet (EEE);
- 8.33.30. Suportar a funcionalidade de Link aggregation (LACP) nas portas de uplink para redundância ou aumento de capacidade;
- 8.33.31. Deve operar em condições de temperatura entre 0°C e 50°C, e humidade entre 5% e 93%;
- 8.33.32. Deve possuir MTBF (Mean Time Between Failure (MTBF) de no mínimo 995.000 (novecentos e noventa e cinco mil) horas;
- 8.33.33. Possuir botão de reset que permita reset de fábrica do equipamento;
- 8.33.34. Possuir porta de console para gerenciamento e configuração via linha de comando CLI;
- 8.33.35. Possuir interface USB2.0;
- 8.33.36. Possuir interface de rádio Bluetooth 5 integrada, com no mínimo as seguintes características:
- 8.33.37. Potência de transmissão no mínimo de 8 dBm (classe 1) e sensibilidade de recepção mínima de -95 dBm;
- 8.33.38. Deve possuir interface IoT (Internet of Things) integrada ao equipamento, com no mínimo as seguintes características:
- 8.33.39. Potência de transmissão no mínimo de 8 dBm e sensibilidade de recepção mínima de -97 dBm;
- 8.33.40. Possuir slot de segurança Kensington;
- 8.33.41. Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação;
- 8.33.42. Possuir kits de montagem opcionais para instalar o AP em variedade de superfícies
- 8.33.43. Deve permitir o gerenciamento através de controladora local e/ou utilizando sistema de gerenciamento em nuvem pública do mesmo fabricante;
- 8.33.44. Deverá gerenciar todas as funcionalidades e regras de WLAN e todos os Pontos de Acesso de forma centralizada;
- 8.33.45. Deve suportar a criação de arquitetura distribuída ou site único de rede sem fio.
- 8.33.46. Deve possuir arquitetura controlada com alta disponibilidade, em caso de falha da

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
controladora principal, um novo controlador deve assumir o papel de controle das funcionalidades da rede WLAN.

- 8.33.47. Deve ser capaz de gerenciar todos os APs baseado em grupo, devendo oferecer suporte a no mínimo 120 APs por grupo.
- 8.33.48. Deve possuir suporte a gerenciamento baseado na web, utilizando os principais navegadores. (Microsoft Internet Explorer, Apple Safari, Google Chrome e Mozilla Firefox)
- 8.33.49. Deve permitir atualizações de firmware e configuração automática;
- 8.33.50. Deve permitir administrar centralizadamente todos os aspectos de segurança da rede WLAN através de firewall integrado ao sistema de rede sem fio;
- 8.33.51. Deve permitir a criação de regras de acesso baseado em aplicação e em categoria de aplicação;
- 8.33.52. Caso o controlador não possua firewall do tipo statefull integrado, poderão ser fornecidos appliances do mesmo fabricante, que contemplem as solicitações e características solicitadas para o firewall;
- 8.33.53. Deve realizar o controle de autorização baseado em perfis de acesso, permitindo no mínimo 32 perfis;
- 8.33.54. Deve permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação;
- 8.33.55. Deve possuir gerenciamento e controle de uso de largura de banda, baseado em taxa de utilização de banda ou perfil de acesso;
- 8.33.56. Deve permitir associar diferentes tipos de privilégios baseado em autenticação de máquina ou autenticação de usuário;
- 8.33.57. Deve suportar configuração de uso de downloadable user ACL (DUR) ou Dynamic ACL (DACL);
- 8.33.58. Gerenciamento Inteligente de potência;
- 8.33.59. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;
- 8.33.60. Permitir habilitar e desabilitar a divulgação do SSID;
- 8.33.61. Permitir habilitar e desabilitar o SSID;
- 8.33.62. Implementar diferentes tipos de combinações encriptação/autenticação por SSID;
- 8.33.63. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.33.64. Suporte a IPv6;
- 8.33.65. Possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas;
- 8.33.66. Possibilitar análise de espectro nos canais em que estiver provendo acesso, sem desconectar os usuários;
- 8.33.67. Implementar VLANs conforme padrão IEEE 802.1Q;
- 8.33.68. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono);
- 8.33.69. Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível;
- 8.33.70. Implementar cliente DHCP para configuração automática de rede;
- 8.33.71. Deve configurar-se automaticamente ao ser conectado na rede;
- 8.33.72. Possuir mecanismo de reconhecimento de aplicações através de DPI (Deep Packet Inspection) permitindo a classificação e bloqueio, priorização de tráfego ou limitação de banda;
- 8.33.73. Possuir mecanismo de prevenção a intrusão em redes WiFi (WIPS) oferecendo proteção contra ameaças e eliminando assim a necessidade de sensores dedicados a esse fim
- 8.33.74. Possuir serviços de reputação e segurança para identificar, classificar e bloquear arquivos, URLs e endereços IP maléficos provendo um mecanismo de proteção compreensivo as ameaças;
- 8.33.75. Implementar varredura de RF nas frequências 2.4GHz e 5GHz, para identificação de interferências em dispositivos Wi-Fi, bem como também em dispositivos não Wi-Fi como Bluetooth, Forno Microondas, Telefone sem Fio, entre outros;
- 8.33.76. Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2;
- 8.33.77. Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;
- 8.33.78. Permitir a integração com LDAP;
- 8.33.79. Implementar WPA com algoritmo de criptografia TKIP e MIC;
- 8.33.80. Implementar WPA2 com algoritmo de criptografia AES 128, IEEE 802.11i;
- 8.33.81. Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CNSA, AES-CCM-256 e SAE-AES;
- 8.33.82. Possuir kits de montagem opcionais para instalar o AP em variedade de

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
superfícies;

- 8.33.83. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
- 8.33.84. O equipamento proposto deverá possuir garantia de 3 (três) anos;
- 8.33.85. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, este item deve ser do mesmo fabricante demais pontos de acesso e do software de controle de acesso de rede descritos neste termo de referência.

#### **8.34. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE PONTO DE ACESSO SEM FIO TIPO 1**

- 8.34.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do ponto de acesso sem fio tipo 1, que compreendem, entre outros, os seguintes procedimentos:
- 8.34.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;
- 8.34.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
- 8.34.4. Conexão do ponto de acesso sem fio tipo 1 na rede de comunicação de dados através de link de dados óptico ou metálico, designado para este fim;
- 8.34.5. Deverá prever a identificação física do ponto de acesso sem fio tipo 1;
- 8.34.6. Devem ser implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades do ponto de acesso sem fio tipo 1 explorando suas características, dentro das melhores práticas de rede de computadores, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação;
- 8.34.7. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados, bem como análise das plantas baixas fornecidos pela CONTRATANTE;
- 8.34.8. Durante a implantação, a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
- 8.34.9. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;

- 8.34.10. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE
- 8.34.11. Devem ser realizados todos os ajustes de hardware e software necessários ao funcionamento dos equipamentos.
- 8.34.12. Todas as atualizações de firmware ou qualquer outro software componente, para a versão mais atualizada disponível ou a última compatível.
- 8.34.13. Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.

**8.35. PONTO DE ACESSO SEM FIO - TIPO 2**

- 8.35.1. Características gerais do equipamento Ponto de Acesso sem fio Tipo 2 a ser fornecido:
- 8.35.2. Equipamento de Ponto de Acesso (AP) Outdoor para rede local sem fio com dois rádios, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac/ax, 5GHz, e IEEE 802.11b/g/n/ax, 2.4GHz;
- 8.35.3. O equipamento deve possuir proteção para ambientes externos, não serão aceitos equipamentos com caixas de proteção genéricas;
- 8.35.4. Deve ser apto a operação outdoor sem utilização de caixa de instalação adicional;
- 8.35.5. Os pontos de acesso deverão possuir certificado emitido pelo “WIFI Alliance” comprovando os seguintes padrões, protocolos e funcionalidades:
- 8.35.6. IEEE 802.11a;
- 8.35.7. IEEE 802.11b;
- 8.35.8. IEEE 802.11g;
- 8.35.9. IEEE 802.11n;
- 8.35.10. IEEE 802.11ac;
- 8.35.11. IEEE 802.11ax;
- 8.35.12. WPA Enterprise/Personal;
- 8.35.13. WPA2 Enterprise/Personal;
- 8.35.14. WPA3 Enterprise/Personal;
- 8.35.15. Passpoint (Release 2)

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.35.16. WMM, WMM-PS (Power Save), Wi-Fi Vantage, Wi-Fi Agile Multiband;
- 8.35.17. Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n, 801.11ac e 802.11ax;
- 8.35.18. Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:
- 8.35.19. 802.11b: 1, 2, 5.5, 11;
- 8.35.20. 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54;
- 8.35.21. 802.11n 6.5 a 300 (MCS0 a MCS15, HT20 a HT40);
- 8.35.22. 802.11ac: 6.5 a 867 (MCS0 a MCS9, NSS = 1 a 2, VHT20 a VHT80);
- 8.35.23. 802.11ax (2.4GHz): 3.6 a 574 (MCS0 a MCS11, NSS = 1 a 2, HE20 a HE40);
- 8.35.24. Deve suportar 802.11n high-throughput (HT): HT20/40;
- 8.35.25. Deve suportar 802.11ac very high throughput (VHT): VHT20/40/80;
- 8.35.26. Deve suportar 802.11ax high efficiency (HE): HE20/40/80;
- 8.35.27. Deve suportar 802.11n/ac packet aggregation: A-MPDU, A-MSDU;
- 8.35.28. Operar nas seguintes tecnologias de rádio:
- 8.35.29. 802.11b: Direct-sequence spread-spectrum (DSSS);
- 8.35.30. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM);
- 8.35.31. 802.11ax: Orthogonal frequency-division multiple access (OFDMA);
- 8.35.32. Operar nos seguintes tipos de modulação:
- 8.35.33. 802.11b: BPSK, QPSK, CCK;
- 8.35.34. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM;
- 8.35.35. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM;
- 8.35.36. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM;
- 8.35.37. Possuir capacidade de selecionar automaticamente o canal de transmissão - DFS;
- 8.35.38. Suportar até 256 clientes associados por rádio;
- 8.35.39. Possuir suporte a pelo menos 16 SSIDs;
- 8.35.40. Possuir 04 (quatro) antenas integradas ao equipamento, com padrão de irradiação omnidirecional, dual-band, com ganho de, pelo menos, 3.0 dBi em 2.4GHz e com ganho de, pelo menos, 5.0 dBi em 5GHz;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.35.41. Deve suportar, utilizando a modulação OFDMA, a capacidade de transmitir simultaneamente clientes por canal;
- 8.35.42. Deve operar em 5GHz 2x2 MIMO;
- 8.35.43. Deve operar em 2.4GHz 2x2 MIMO;
- 8.35.44. Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas;
- 8.35.45. Possuir potência máxima de transmissão para frequências de 2.4GHz de no mínimo: +23 dBm;
- 8.35.46. Possuir potência máxima de transmissão para frequências de 5GHz de no mínimo: +23 dBm;
- 8.35.47. Capacidade de configurar a potência de transmissão em incrementos de 0.5 dBm;
- 8.35.48. Deve permitir funcionamento em modo gerenciado por controladora, para otimização de performance de rede, roaming, segurança, todos os Pontos de Acesso criam um túnel com todo tráfego centralizado para o gerenciamento;
- 8.35.49. Deve permitir funcionamento em modo auto gerenciado, sem a necessidade de uma controladora WLAN, onde o próprio Ponto de Acesso pode operar como um Controladora Virtual.
- 8.35.50. Deve permitir o gerenciamento através de plataforma nuvem (cloud).
- 8.35.51. Deve permitir o gerenciamento através de plataforma local (on-premise).
- 8.35.52. Para implementações em larga escala, o Ponto de Acesso deve configurar-se automaticamente ao ser conectado na rede, sendo provisionado através da ferramenta de gerenciamento;
- 8.35.53. Possuir LED's multicoloridos indicativos do estado de operação e da atividade do rádio;
- 8.35.54. Deve possuir 01 (uma) interface de rede 10/100/1000BASE-T Ethernet (RJ-45) com as seguintes características:
  - 8.35.55. Auto-sensing link speed e MDI/MDX;
  - 8.35.56. 802.3az Energy Efficient Ethernet (EEE);
  - 8.35.57. Deve operar em condições de temperatura entre 0°C e 50°C, e umidade entre 5% e 93%;
  - 8.35.58. Possuir botão de reset que permita reset de fábrica do equipamento;
  - 8.35.59. Possuir porta de console para gerenciamento e configuração via linha de comando CLI;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.35.60. Possuir interface USB2.0;
- 8.35.61. Possuir interface de rádio Bluetooth 5 integrada, com no mínimo as seguintes características:
- 8.35.62. Potência de transmissão no mínimo de 8 dBm (classe 1) e sensibilidade de recepção mínima de -95 dBm;
- 8.35.63. Deve possuir interface Zigbee integrada ao equipamento, com no mínimo as seguintes características:
- 8.35.64. Potência de transmissão no mínimo de 8 dBm e sensibilidade de recepção mínima de -97 dBm;
- 8.35.65. Possuir slot de segurança Kensington;
- 8.35.66. Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação;
- 8.35.67. Possuir kits de montagem opcionais para instalar o AP em variedade de superfícies;
- 8.35.68. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
- 8.35.69. O equipamento proposto deverá possuir garantia de 3 (três) anos;
- 8.35.70. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este equipamento, por questões de compatibilidade, gerência, suporte e garantia, este item deve ser do mesmo fabricante demais pontos de acesso e do software de controle de acesso de rede descritos neste termo de referência

**8.36. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE PONTO DE ACESSO SEM FIO TIPO 2**

- 8.36.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do ponto de acesso sem fio tipo 2, que compreendem, entre outros, os seguintes procedimentos:
- 8.36.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;
- 8.36.3. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);
- 8.36.4. Conexão do ponto de acesso sem fio tipo 2 na rede de comunicação de dados através de link de dados óptico ou metálico, designado para este fim;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.36.5. Deverá prever a identificação física do ponto de acesso sem fio tipo 2;
- 8.36.6. Devem ser implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades do ponto de acesso sem fio tipo 2 explorando suas características, dentro das melhores práticas de rede de computadores, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação;
- 8.36.7. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados, bem como análise das plantas baixas fornecidos pela CONTRATANTE;
- 8.36.8. Durante a implantação a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados;
- 8.36.9. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
- 8.36.10. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE
- 8.36.11. Devem ser realizados todos os ajustes de hardware e software necessários ao funcionamento dos equipamentos.
- 8.36.12. Todas as atualizações de firmware ou qualquer outro software componente, para a versão mais atualizada disponível ou a última compatível.
- 8.36.13. Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.
- 8.37. GERENCIAMENTO UNIFICADO DE INFRAESTRUTURA DE REDE LAN E WLAN, CONTROLE DE ACESSO DE USUÁRIOS WIRELESS, ORQUESTRAÇÃO E APROVISIONAMENTO AUTOMÁTICO.**
- 8.37.1. Deverá ser fornecido serviço de gerenciamento de infraestrutura de switches e pontos de acesso por software que atenda as seguintes características mínimas:
- 8.37.2. O sistema de gerenciamento deve ser acessado através de provedores de nuvem pública, sem depender de instalações locais de software ou Hardware para o seu funcionamento.
- 8.37.3. As funcionalidades descritas deverão ser providas no modelo SaaS (Software as a Service), como serviço, ou seja, todos os recursos de Hardware, Software, suporte, manutenção e segurança, para funcionamento do item proposto deverão ser providos pelo fornecedor.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.37.4. O sistema de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL v1.3.
- 8.37.5. Todo acesso deverá ser controlado com autenticação de usuário em base própria também externa utilizando para isso Single-Sign-on através do protocolo SAML.
- 8.37.6. Os privilégios de acesso deverão ser controlados através de RBAC (Role Base Access Control) permitindo derivar privilégios por usuário baseado em Roles para determinar quais níveis de acesso será permitido.
- 8.37.7. O sistema de gerenciamento deverá prover tutoriais interativos como guia para acesso as facilidades básicas, incluindo no mínimo, criação de usuários e roles, configuração e gestão de redes, monitoramento de equipamentos e redes, diagnósticos e interface de usuário.
- 8.37.8. O sistema de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para Access Points e Switches, através de um único painel.
- 8.37.9. Toda a comunicação entre o sistema de gerenciamento e os dispositivos gerenciados deverá ser feita através de conexão segura SSL v1.3, utilizando porta TCP 443.
- Os certificados digitais utilizados para estabelecimento desta comunicação segura deverão estar armazenados em hardware específicos (TPM - Trusted Platform Module) nos dispositivos a serem gerenciados.
- As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas.
- 8.37.10. O sistema de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário.
- 8.37.11. O sistema de gerenciamento deve permitir o licenciamento de dispositivos a serem gerenciados pelo período de 03 (três) anos.
- 8.37.12. Deve permitir que as licenças sejam migradas entre equipamentos da mesma família, para o caso de substituição de equipamentos com defeito ou outros, sem depender de abertura de chamado técnico para isso.
- 8.37.13. Deve contemplar todas as atualizações disponibilizadas de maneira automática durante o período de vigência das licenças, sem depender de intervenção manual do operador.
- 8.37.14. Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play), específico para a implantação de uma nova localidade, permitindo a ativação de switches e Access Points.

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

A utilização do aplicativo para ativação deverá ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada.

O aplicativo para ativação deverá permitir o envio de foto para comprovar o término da implantação pelo usuário, além de permitir o envio de instruções básicas para o instalador através do painel de acompanhamento e gestão da implantação.

Após marcada como concluída, ou finalizado o período para implantação, o usuário do aplicativo não terá mais acesso a referida rotina para implantação.

Toda a configuração, bem como a versão de software em que os equipamentos deverão utilizar, deverão ser automaticamente enviadas após a conclusão da implantação através do aplicativo.

8.37.15. Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso ao sistema de gerenciamento, nos casos onde não houver serviço de configuração dinâmica de endereços IPs para acesso à Internet.

8.37.16. Todo o sistema de gerenciamento deverá estar disponível em Português, permitindo alternar para o Inglês conforme desejado pelo operador.

8.37.17. O sistema de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso WI-FI.

As configurações do grupo ao qual o equipamento está associado deverão ser substituídas pelas configurações associadas ao equipamento específico (interfaces, VLAN, endereçamento IP, gateway, hostname)

Os grupos devem permitir dois modos de configuração dos equipamentos, interface gráfica e através de templates em arquivos de linha de comando.

8.37.18. Os arquivos templates em linha de comando deverão permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração

8.37.19. Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento

8.37.20. Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino

8.37.21. Deverá permitir que as configurações sejam salvas através de acesso direto ao equipamento (switch e AP) via FTP, SFTP e TFTP.

8.37.22. Deverá promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos (Switches e AP), sem necessidade de acesso local

8.37.23. Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.37.24. Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade
- 8.37.25. Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução
- 8.37.26. Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração ao sistema de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos
- 8.37.27. Deverá possuir Streaming API, que permita o envio de informações a partir do sistema de gerenciamento sem depender de requisições externas, entre elas:

Auditoria (conexão, configuração e firmware de equipamentos)

Localização (coordenadas de localização de clientes WI-FI)

Fluxo de sessões (sessões WEB dos clientes conectados através do WI-FI)

Monitoramento (status e estatísticas) de clientes

Presença (detalhes de clientes conectados e não conectados a rede WI-FI)

Segurança (reportar alertas de WIDS)"

"Deverá permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:

Alertas de Usuários

Alertas de Pontos de Acesso WI-FI

Alertas de Switches

Alertas de conectividade com o sistema de gerência

Alertas de auditoria

Alertas de localidade"

Deverá identificar o dispositivo conectado a rede através da rede WI-FI, expondo os seguintes parâmetros:

Categoria

Família

Sistema Operacional

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Atributos de fluxo de tráfego por dispositivo:

Destinos acessados e host de destino

Aplicações e grupos de aplicações"

8.37.28. Deverá permitir a integração, através de API, com sistema que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.

8.37.29. Funcionalidade de análise de presença (Presence Analytics), de forma a permitir:

Obtenção de informações em tempo real e baseado em dados históricos, de quantos clientes potenciais passaram pela área de cobertura, quantos entraram, quantos se conectaram e qual o tempo médio de permanência na área de cobertura;

Realizar comparações de métricas por múltiplas localidades

Permitir a customização de níveis de potência de sinal (RSSI) e limiares de tempo para medir o tráfego e realizar as categorizações;

Caso seja utilizado sistema de terceiros para análise de presença (Presence Analytics), estas devem ser homologadas pelo fornecedor dos equipamentos de rede;"

8.37.30. Funcionalidade de relatórios:

Capacidade de geração de relatório para armazenagem de informações;

Coleta de informações da rede por períodos de tempo pré-definidos;

Capacidade de geração e envio automático de relatórios por e-mail;

Caso seja utilizado sistema de terceiros para a geração de relatórios, estas devem ser homologadas pela pelo fornecedor dos equipamentos de rede."

8.37.31. Funcionalidade de Gerenciamento de Convidados (Guests)

Deve possuir recurso de gerenciamento de convidados permite que os usuários convidados se conectem à rede e, ao mesmo tempo, permite que o administrador controle o acesso dos usuários convidados à rede.

Os administradores podem criar um perfil de página inicial para seus usuários convidados.

Deve permitir a personalização do layout da página inicial (vertical ou horizontal) com base no tipo de dispositivo.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Permitir que os convidados acessem a Internet fornecendo as credenciais configuradas pelos operadores convidados ou suas respectivas credenciais de login na rede social.

Permitir acesso utilizando logins sociais das redes Facebook, Google, Twitter, and LinkedIn.

Deve permitir o serviço Wi-Fi do Facebook, de forma que os usuários que se conectam a hotspots Wi-Fi sejam apresentados a uma página de negócios antes de obter acesso à rede.

- 8.37.32. A ferramenta deve ter capacidade de criar uma conta com permissão apenas de poder criar contas de usuários da rede Wi-Fi sem que tenha acesso as configurações dos elementos de rede ou outros serviços.
- 8.37.33. Permitir a criação de contas de usuários da rede Wi-Fi com prazos de tempo.
- 8.37.34. Deve permitir que os visitantes ou usuários convidados podem se registrar usando a página inicial ao tentar acessar a rede. A senha é entregue aos usuários por meio de impressão, SMS ou e-mail dependendo das opções selecionadas durante o cadastro.
- 8.37.35. Deve fornecer as credenciais de login por meio de impressão, mensagens de texto SMS ou e-mail.
- 8.37.36. O Controle de acesso de rede deverá possuir os seguintes requisitos mínimos.
- 8.37.37. Sistema de autenticação de usuários e dispositivos para controle de acesso a rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors: VmWare ESXi 5.5 ou superior, Microsoft Hyper-V Server 2012 R2/2016 e Windows Server 2012 R2 com Hyper-V, Amazon EC2, CentOS KVM;"
- 8.37.38. Suporte a seguintes fontes para autenticação: Microsoft Active Directory, Kerberos, LDAP-compliant directory, ODBC-compliant SQL server, Token servers, Base SQL interna, Radius, Microsoft Azure Active Directory, Google G Suite, HTTP, Lista estática de endereços MAC;
- 8.37.39. Deve suportar "Single Sign-on" (SSO) através de SAML v2.0;
- 8.37.40. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em: Atributos do usuário autenticado, Hora do dia, dia da semana, Tipo de dispositivo utilizado, Localização do usuário, Tipo de autenticação utilizado;
- 8.37.41. Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

protocolo utilizados na requisição (ex. RADIUS), informações de resposta do sistema para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise;

- 8.37.42. Deve possuir Dashboard customizável, que permita a visualização de no mínimo as seguintes informações:
- 8.37.43. Lista com os últimos Alertas do sistema;
- 8.37.44. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;
- 8.37.45. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;
- 8.37.46. Para sistema compostas por mais de um servidor/appliance, deve apresentar o Status de cada elemento dos sistemas, com informações como endereço IP e data da última replicação dos dados;
- 8.37.47. Gráfico com a categorização dos dispositivos classificados pelo sistema, divididos de acordo com as categorias de classificação;
- 8.37.48. Últimas falhas de autenticação;
- 8.37.49. Lista com as últimas autenticações;
- 8.37.50. Lista com as últimas autenticações com sucesso;
- 8.37.51. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;
- 8.37.52. Deve implementar funcionalidade de classificação automática de dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
- 8.37.53. Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc.);
- 8.37.54. Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;
- 8.37.55. Deve possuir base de regras e categorias de dispositivos pré-configurada;
- 8.37.56. Deve suportar mecanismo de atualização das regras e categorias pré-configuradas;
- 8.37.57. Deve possuir suporte a RADIUS CoA, Web authentication e SAML v2.0;
- 8.37.58. Deve suportar no mínimo os seguintes métodos de autenticação:
- 8.37.59. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.37.60. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD);
- 8.37.61. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);
- 8.37.62. EAP-TLS;
- 8.37.63. PAP, CHAP, MSCHAPv1, MSCHAPv2, e EAP-MD5;
- 8.37.64. Windows machine authentication;
- 8.37.65. SMB v2/v3;
- 8.37.66. WPA3 – MPSK;
- 8.37.67. RADSec;
- 8.37.68. Online Certificate Status Protocol (OCSP);
- 8.37.69. TACACS+ Server;
- 8.37.70. WEB Authentication;
- 8.37.71. Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS TCP na camada de transporte, utilizando TLS para encriptação da comunicação;
- 8.37.72. Deve possuir suporte à integração com plataforma de terceiros usando HTTP/RESTful API;
- 8.37.73. Deve permitir que o sistema faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
- 8.37.74. Deve possuir suporte aos seguintes recursos através de IPv6:
- 8.37.75. Administração via WEB e CLI;
- 8.37.76. Servidores de autenticação e autorização com endereçamento IPv6;
- 8.37.77. IPv6 Accounting Proxy;
- 8.37.78. Acesso a servidores com endereçamento IPv6 para contexto de endpoints;
- 8.37.79. Syslog, DNS, NTP;
- 8.37.80. Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;
- 8.37.81. Fontes de Syslog para processamento de eventos;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.37.82. Validações e conformidades;
- 8.37.83. FIPS 140-2;
- 8.37.84. Common Criteria NDcPP + Servidor de autenticação;
- 8.37.85. Deve permitir configuração em alta disponibilidade com no mínimo dois elementos, sendo que ambos devem permanecer ativos para o processamento das requisições;
- 8.37.86. Deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam a mesma "zona";
- 8.37.87. Deve permitir a geração e o envio através de e-mail ou SMS de alertas relativos as seguintes atividades anormais detectadas na rede:
- 8.37.88. Autenticações;
- 8.37.89. Acesso a dispositivos de rede;
- 8.37.90. Tentativa de execução de comandos em dispositivos de rede por usuários sem privilégios;
- 8.37.91. Atividades irregulares nos servidores do serviço;
- 8.37.92. Deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF;
- 8.37.93. Deve suportar recurso de alta disponibilidade (HA) do tipo Ativo + Ativo. Todas as licenças necessárias para esta funcionalidade devem ser fornecidas;
- 8.37.94. O item proposto deverá ser ofertada com licenciamento para 1000 (um mil) usuários no modelo de autenticação para 802.1X, Autenticação via MAC, Autenticação via WEB e autenticação via portal;
- 8.37.95. O item proposto deverá estar licenciada para o serviço de servidor TACACs para 1000 (um mil) dispositivos;
- 8.37.96. Deve implementar os serviços de autenticação, profiling e autorização para 1000 (um mil) usuários/dispositivos;
- 8.37.97. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), este sistema e software, para fins de padronização, otimização de recursos, compatibilidade, gerência, garantia de fabricante, suporte e garantia de perfeita interoperabilidade e melhor otimização dos recursos disponíveis, este item deve ser do mesmo fabricante dos pontos de acesso e switches descritos neste termo de referência.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

**8.38. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE GERENCIAMENTO UNIFICADO DE INFRAESTRUTURA DE REDE LAN E WLAN, CONTROLE DE ACESSO DE USUÁRIOS WIRELESS, ORQUESTRAÇÃO E APROVISIONAMENTO AUTOMÁTICO.**

- 8.38.1. A CONTRATADA deverá prestar serviços de planejamento, instalação e configuração do gerenciamento unificado de infraestrutura de rede lan e wlan, controle de acesso de usuários wireless, orquestração e provisionamento automático, que compreendem, entre outros, os seguintes procedimentos:
- 8.38.2. Reuniões de alinhamento para criação do escopo do projeto previamente a instalação;
- 8.38.3. Ativação e Instalação de licenças (softwares), conforme equipamentos definidos nesta especificação.
- 8.38.4. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;
- 8.38.5. Durante a implantação a equipe da CONTRATADA deverá repassar as informações para a equipe da CONTRATANTE apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados e será firmado termo de sigilo entre as partes;
- 8.38.6. O processo de implantação deverá ser devidamente documentado pela CONTRATADA, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação contendo todas as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;
- 8.38.7. Devem ser realizados todos os ajustes de hardware e software necessários para que todos os equipamentos cadastrados possam ser gerenciados.
- 8.38.8. Instalação de todas as atualizações de firmware ou qualquer outro software componente, para a versão mais atualizada disponível ou a última compatível.

**8.39. CÂMERA IP - TIPO 1**

- 8.39.1. Características mínimas da câmera IP Tipo 1 a ser fornecida:
- 8.39.2. Câmera tipo Dome;
- 8.39.3. Possuir resolução mínima de 2 (dois) Mega Pixels (1920 × 1080), operando com uma taxa mínima de 30 (trinta) quadros por segundo;
- 8.39.4. Possuir sensor de imagem CMOS 1/2.8" ou maior, com varredura progressiva;
- 8.39.5. Possuir obturador com velocidade de 1/3s a 1/100.000s;
- 8.39.6. Possuir suporte para 3 (três) fluxos de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo;
- 8.39.7. Possuir capacidade de operar em baixa luminosidade com sensibilidade mínima

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
de 0.01 Lux, em modo colorido, AGC ligado e 0 (zero) Lux com IR acionado;

- 8.39.8. Possuir iluminadores IR integrados, com alcance mínimo de 40 (quarenta) metros;
- 8.39.9. Possuir lente varifocal integrada de 2.8 a 12mm, com ângulo de visualização horizontal mínimo de 110°;
- 8.39.10. Possuir no mínimo 1 (uma) entrada e 1 (uma) saída de áudio, com suporte aos codecs de áudio: G.711 e G.726;
- 8.39.11. Possuir no mínimo 1 (uma) entrada e 1 (uma) saída de alarme;
- 8.39.12. Possuir WDR com ampla faixa dinâmica de 120 dB, não será aceito WDR digital;
- 8.39.13. Possuir recurso que permita a inclusão de máscaras de privacidade;
- 8.39.14. Possuir função de rotação com inversão da proporção do aspecto de imagem (modo corredor);
- 8.39.15. Possuir proteção total contra poeira e jatos fortes d'água – grau de proteção IP66 ou superior;
- 8.39.16. Possuir proteção total contra vandalismo e impactos – grau de proteção IK10 ou superior;
- 8.39.17. Possuir alimentação compatível para 12Vdc e PoE (802.3af);
- 8.39.18. Possuir compressão de vídeo padrão H.264 e, ao menos, um padrão de compressão de vídeo superior ao mesmo (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares), com alta relação de compressão;
- 8.39.19. Possuir função Dia & Noite com filtro de IR com troca automática;
- 8.39.20. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente nesta área a imagem possua a resolução máxima configurada na câmera;
- 8.39.21. Possuir funções BLC (Compensação de Luz de Fundo), 3D-DNR (Redução Digital de ruídos - 3D) e HLC (Compensação de Luz Forte);
- 8.39.22. Possuir função de obturador lento, que mantem a nitidez da imagem quando ocorre queda da iluminação do ambiente;
- 8.39.23. Possuir interface web no idioma Português (Brasil);
- 8.39.24. Possuir compatibilidade com padrão ONVIF (Profile T), deve estar presente no site do fórum mundial ONVIF como uma câmera homologada.  
<https://www.onvif.org/conformant-products/>;
- 8.39.25. Possuir arquitetura aberta para integração com outros sistemas;

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

- 8.39.26. Possuir compatibilidade com os protocolos de rede: TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, QoS, IPv6;
- 8.39.27. Possuir suporte a NAS para armazenamento na rede;
- 8.39.28. Possuir a capacidade de detectar e gerar alerta dos seguintes eventos: detecção de movimento, violação de vídeo, desconexão de rede, conflito de endereço IP, armazenamento local cheio, tentativa de login irregular e armazenamento local com erro;
- 8.39.29. Possuir slot para cartão micro SD/SDHC/SDXC com capacidade de até 128GB;
- 8.39.30. Possuir recurso de gravação automática no cartão em caso de perda de conexão com o software VMS;
- 8.39.31. Possuir conexão RJ45 10/100M auto adaptável;
- 8.39.32. Possuir capacidade de operar em temperaturas de -20 °C ~ 60 °C com humidade não superior a 95% (sem condensação);
- 8.39.33. Deve ser fornecida com cartão memória para armazenamento de no mínimo 32 GB, classe 10;
- 8.39.34. Deve ser fornecida com suporte, no qual seja possível acomodar cabos e conexões da câmera de maneira que não fiquem aparentes, para fixação em parede, teto ou poste, conforme a necessidade e local de instalação;
- 8.39.35. Deve ser compatível com o software VMS descrito neste termo de referência;
- 8.39.36. Deve possuir garantia mínima de 3 (três) anos;

**8.40. CÂMERA IP - TIPO 2**

- 8.40.1. Características mínimas da câmera IP Tipo 2 a ser fornecida:
- 8.40.2. Câmera tipo Mini Bullet;
- 8.40.3. Resolução mínima de 2 (dois) Mega Pixels (1920 x 1080) operando com uma taxa mínima de 30 quadros por segundo;
- 8.40.4. Deve possuir sensor de imagem CMOS 1/2.8" ou maior, com varredura progressiva;
- 8.40.5. Possuir suporte para 3 (três) fluxos de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo;
- 8.40.6. Possuir capacidade de operar em baixa luminosidade com sensibilidade mínima de 0.009 Lux, em modo colorido, AGC ligado e 0 (zero) Lux com IR acionado;
- 8.40.7. Possuir iluminadores IR integrados, com alcance mínimo de 30 (trinta) metros;
- 8.40.8. Possuir lente de 2.8mm com ângulo de visão de no mínimo 105°;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.40.9. Possuir função de rotação com inversão da proporção do aspecto de imagem (modo corredor);
- 8.40.10. Possuir WDR com ampla faixa dinâmica de 120 dB, não será aceito WDR digital;
- 8.40.11. Possuir funções inteligentes de análise de vídeo para: detecção de cruzamento de linha, detecção de intrusos em uma determinada área, detecção de movimentos, detecção de obstrução de vídeo, detecção de objeto abandonado, detecção de objeto removido;
- 8.40.12. Possuir proteção total contra poeira e jatos fortes d'água – grau de proteção IP67 ou superior;
- 8.40.13. Possuir alimentação compatível para 12Vdc e PoE (802.3af);
- 8.40.14. Possuir compressão de vídeo padrão H.264 e, ao menos, um padrão de compressão de vídeo superior ao mesmo (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares), com alta relação de compressão;
- 8.40.15. Possuir função Dia & Noite com filtro de IR com troca automática;
- 8.40.16. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente nesta área a imagem possua a resolução máxima configurada na câmera;
- 8.40.17. Possuir funções BLC (Compensação de Luz de Fundo), 3D-DNR (Redução Digital de ruídos - 3D) e HLC (Compensação de Luz Forte);
- 8.40.18. Possuir função de obturador lento, que mantém a nitidez da imagem quando ocorre queda da iluminação do ambiente;
- 8.40.19. Possuir interface web no idioma Português (Brasil);
- 8.40.20. Possuir compatibilidade com padrão ONVIF (Profile T), deve estar presente no site do fórum mundial ONVIF como uma câmera homologada.  
<https://www.onvif.org/conformant-products/>;
- 8.40.21. Possuir arquitetura aberta para integração com outros sistemas;
- 8.40.22. Possuir compatibilidade com os protocolos de rede: TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, QoS, IPv6;
- 8.40.23. Possuir suporte a NAS para armazenamento na rede;
- 8.40.24. Possuir a capacidade de detectar e gerar alerta dos seguintes eventos: detecção de movimento, violação de vídeo, desconexão de rede, conflito de endereço IP, armazenamento local cheio, tentativa de login irregular e armazenamento local com erro;
- 8.40.25. Possuir slot para cartão micro SD/SDHC/SDXC com capacidade de até 128GB;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.40.26. Possuir recurso de gravação automática no cartão em caso de perda de conexão com o software VMS;
- 8.40.27. Possuir conexão RJ45 10/100M auto adaptável;
- 8.40.28. Possuir capacidade de operar em temperaturas de -20 °C ~ 60 °C com humidade não superior a 95% (sem condensação);
- 8.40.29. Deve ser fornecida com cartão memória para armazenamento de no mínimo 32 GB, classe 10;
- 8.40.30. Deve ser fornecida com suporte, no qual seja possível acomodar cabos e conexões da câmera de maneira que não fiquem aparentes, para fixação em parede, teto ou poste, conforme a necessidade e local de instalação;
- 8.40.31. Deve ser compatível com o software VMS descrito neste termo de referência;
- 8.40.32. Deve possuir garantia mínima de 3 (três) anos;

**8.41. CÂMERA IP - TIPO 3**

- 8.41.1. Características mínimas da câmera IP Tipo 3 a ser fornecida:
- 8.41.2. Câmera tipo Bullet;
- 8.41.3. Possuir resolução mínima de 4 (quatro) Mega Pixels (2688 × 1520) operando com uma taxa mínima de 30 quadros por segundo;
- 8.41.4. Possuir sensor de imagem CMOS 1/2.5" ou maior, com varredura progressiva;
- 8.41.5. Possuir suporte para 3 (três) fluxos de vídeo independentes e configuráveis em resolução e taxa de quadros por segundo;
- 8.41.6. Possuir capacidade de operar em baixa luminosidade com sensibilidade mínima de 0.009 Lux, em modo colorido, AGC ligado e 0 (zero) Lux com IR acionado;
- 8.41.7. Possuir iluminadores IR integrados, com alcance mínimo de 50 (cinquenta) metros;
- 8.41.8. Possuir lente de 2.8mm com ângulo de visão de no mínimo 105°;
- 8.41.9. Possuir função de rotação com inversão da proporção do aspecto de imagem (modo corredor);
- 8.41.10. Possuir WDR com ampla faixa dinâmica de 120 dB, não será aceito WDR digital;
- 8.41.11. Possuir funções inteligentes de análise de vídeo para: detecção de cruzamento de linha, detecção de intrusos em uma determinada área, detecção de movimentos, detecção de obstrução de vídeo, detecção de objeto abandonado, detecção de objeto removido;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.41.12. Possuir proteção total contra poeira e jatos fortes d'água – grau de proteção IP67 ou superior;
- 8.41.13. Possuir alimentação compatível para 12Vdc e PoE (802.3af);
- 8.41.14. Possuir compressão de vídeo padrão H.264 e, ao menos, um padrão de compressão de vídeo superior ao mesmo (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares), com alta relação de compressão;
- 8.41.15. Possuir função Dia & Noite com filtro de IR com troca automática;
- 8.41.16. Possuir função de codificação diferenciada em área marcada da câmera, de modo que somente nesta área a imagem possua a resolução máxima configurada na câmera;
- 8.41.17. Possuir funções BLC (Compensação de Luz de Fundo), 3D-DNR (Redução Digital de ruídos - 3D) e HLC (Compensação de Luz Forte);
- 8.41.18. Possuir função de obturador lento, que mantém a nitidez da imagem quando ocorre queda da iluminação do ambiente;
- 8.41.19. Possuir interface web no idioma Português (Brasil);
- 8.41.20. Possuir compatibilidade com padrão ONVIF (Profile T), deve estar presente no site do fórum mundial ONVIF como uma câmera homologada.  
<https://www.onvif.org/conformant-products/>;
- 8.41.21. Possuir arquitetura aberta para integração com outros sistemas;
- 8.41.22. Possuir compatibilidade com os protocolos de rede: TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, QoS, IPv6;
- 8.41.23. Possuir suporte a NAS para armazenamento na rede;
- 8.41.24. Possuir a capacidade de detectar e gerar alerta dos seguintes eventos: detecção de movimento, violação de vídeo, desconexão de rede, conflito de endereço IP, armazenamento local cheio, tentativa de login irregular e armazenamento local com erro;
- 8.41.25. Possuir slot para cartão micro SD/SDHC/SDXC com capacidade de até 128GB;
- 8.41.26. Possuir recurso de gravação automática no cartão em caso de perda de conexão com o software VMS;
- 8.41.27. Possuir conexão RJ45 10/100M auto adaptável;
- 8.41.28. Possuir capacidade de operar em temperaturas de -20 °C ~ 60 °C com humidade não superior a 95% (sem condensação);
- 8.41.29. Deve ser fornecida com cartão memória para armazenamento de no mínimo 32

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
GB, classe 10;

- 8.41.30. Deve ser fornecida com suporte, no qual seja possível acomodar cabos e conexões da câmera de maneira que não fiquem aparentes, para fixação em parede, teto ou poste, conforme a necessidade e local de instalação;
- 8.41.31. Deve ser compatível com o software VMS descrito neste termo de referência;
- 8.41.32. Deve possuir garantia mínima de 3 (três) anos;

#### **8.42. CÂMERA IP - TIPO 4**

- 8.42.1. Câmera em formato turret lente fixa interna de 2MP com IR de 15m e Video Análise, onde deverá possuir no mínimo as seguintes características:
- 8.42.2. Possuir sensor CMOS de 1/2.8" ou maior, com varredura progressiva, com operação Dia/Noite, através de filtro de infra-vermelho mecânico;
- 8.42.3. Deve possibilitar ajuste do ângulo de visualização horizontal e vertical de pelo menos:
- 8.42.4. 107° x 57° (HxV) com lente fixa de 2,8mm
- 8.42.5. Possuir resolução de 2MP pixels ativos em NTSC 16:9 e 9:16 a 30FPS;
- 8.42.6. Caixa de proteção robusta de alumínio;
- 8.42.7. Suportar ajuste manual de pan/tilt/roll, sendo:
- 8.42.8. Pan: 0° to 350°
- 8.42.9. Tilt: 0° to 78°
- 8.42.10. Roll: 0° to 360°
- 8.42.11. Suportar áudio bidirecional e possuir microfone integrado na câmera. Caso a câmera não possua microfone integrado na mesma, será aceito microfone externo conectado à câmera, para captação do áudio local com as seguintes características mínimas:
- 8.42.12. Transdutor: Condensador de eletreto
- 8.42.13. Padrão polar: Omnidirecional
- 8.42.14. Frequência Faixa: 65Hz ~ 18KHz
- 8.42.15. Sinal / ruído: 74dB SPL
- 8.42.16. Sensibilidade: -30dB +/- 3 dB / 0dB = 1V / Pa, 1kHz
- 8.42.17. Impedância de saída: 1000 ohm ou menos;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.42.18. Suportar protocolos: IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, Telnet, ARP, DHCP, SNMP, SNMP (V1, MIB-II), 802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, CHAP, Digest Authentication.
- 8.42.19. Conexão Ethernet 10/100 Base-T, auto-sensing, half/full duplex, RJ45
- 8.42.20. Suportar operação com compressão H264 e H.265 com qualidade de 2MP a velocidade de 30fps
- 8.42.21. Deve estar em conformidade com a especificação ONVIF Profile S, G e T.
- 8.42.22. Deve implementar formato de compressão de vídeo em H.264, H.265 e M-JPEG, e possuir largura de banda configurável em H.265;
- 8.42.23. Deve permitir transmissão simultânea de pelo menos dois streams de vídeo em H265;
- 8.42.24. Suportar iluminação de 15m de alcance com LED infravermelho de 850nm embutidos e de acionamento automático;
- 8.42.25. Suportar alimentação 12 VDC e PoE (IEEE 802.3af);
- 8.42.26. Suporte obturador de 1/30 a 1/15.000 seg
- 8.42.27. Deve possuir sensibilidade igual ou inferior a no modo colorido a 0,06 lux e no modo monocromático a 0,015 lux (0,0 lux com IR ligado). Estes níveis de sensibilidade devem ser obtidos de acordo com a norma IEC 62676-5 ou similar de mesma capacidade técnica de medição;
- 8.42.28. Possuir WDR real (T-WDR) mínimo de 100dB de acordo com a norma IEC 62676-5 ou similar de mesma capacidade técnica de medição e ainda que comprove a qualidade do processamento de WDR pelo sensor e não por software embarcado na câmera. Não será aceito câmera com WDR processado digitalmente;
- 8.42.29. Classificação contra impactos IK08 para caixa e proteção da lente.
- 8.42.30. Deve possibilitar operação no range de temperatura de -20°C até 50°C;
- 8.42.31. Deve permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no web site do mesmo;
- 8.42.32. A câmera deve possuir botão físico de reset incorporado no hardware da câmera, acessível pelo lado externo da câmera, ou interno, desde que protegido por algum tipo de tampa ou cúpula/domo, sem a necessidade de abertura da caixa da câmera ou que viole o selo de garantia da mesma, evitando-se o contato com o circuito eletrônico interno. O uso do botão de reset deve proporcionar segurança física local para restauração aos padrões de fábrica;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.42.33. Deve possuir recurso integrado de criptografia para o armazenamento em cartão de memória local das imagens;
- 8.42.34. Deve ser fornecido cartão de memória tipo industrial para slot para armazenamento local na câmera do tipo SD/MicroSD card com as seguintes características mínimas:
- 8.42.35. Possuir tecnologia de memória flash MLC NAN com Classe de Velocidade 10, suportando velocidade de leitura de 95MB/s e de gravação de 60MB/s. Deve suportar temperatura de operação de -25°C a +85°C.
- 8.42.36. O cartão de memória deve ser dimensionado para retenção local de imagens por período mínimo de 5 dias, na resolução máxima da câmera (2MP), em 5fps e gravação contínua 24h/dia, considerando até 60% do tempo em cena de baixa movimentação (cena estática) e 40% em alta movimentação (alto tráfego, bitrate máximo da câmera).
- 8.42.37. Apresentar juntamente com a documentação de habilitação técnica a memória de cálculo deste armazenamento em ferramenta oficial do fabricante, e garantido na fase de testes e comissionamento;
- 8.42.38. Deve possuir recurso de análise de vídeo embarcada na câmera e possibilitar o uso simultâneo de no mínimo 6 (seis) algoritmos diferentes.
- 8.42.39. Caso a câmera não possua capacidade incorporada de processamento de 6 algoritmos diferentes simultâneos, será aceita sistema de análise de vídeo baseada em servidor externo, desde que o mesmo possua performance suficiente para executar no mínimo 6 (seis) algoritmos simultâneos por câmera 24h/dia, com licenciamento para o total de câmeras com este recurso solicitado.
- 8.42.40. Catálogo e descritivo técnico do item proposto baseado em servidor externo deverá ser apresentado juntamente com a documentação de comprovação técnica dos demais itens.
- 8.42.41. Deve ser integrada e homologada pelo fabricante do sistema de gerenciamento de vídeo ofertada.
- 8.42.42. Deve ser baseado em servidor deve possuir recurso ativo de busca forense nas imagens gravadas e armazenadas com base nos mesmos algoritmos mínimos solicitados.
- 8.42.43. A câmera ou o sistema e software externo de vídeo análise deve possuir disponibilidade para no mínimo os seguintes algoritmos de análise de vídeo:
- 8.42.44. Detectar objetos na área, e/ou entrando, e/ou saindo de uma área
- 8.42.45. Detectar cruzamento de 3 linhas virtuais, combinadas em lógica e/ou;
- 8.42.46. Detectar objetos através de uma rota;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.42.47. Detectar permanência prolongada de pessoa em uma área em função do raio e do tempo;
- 8.42.48. Detectar objetos deixados por um determinado tempo;
- 8.42.49. Detectar objetos removidos;
- 8.42.50. Detectar objetos com determinadas características como: tamanho, velocidade, direção, cor e mudança de relação de aspecto em um tempo determinado (por exemplo, alguém caindo no chão);
- 8.42.51. Contar objetos cruzando uma linha virtual;
- 8.42.52. Contar objetos em uma área e alarmar se um limite pré definido for atingido;
- 8.42.53. Detectar nível de ocupação (multidão) em uma área pré-definida;
- 8.42.54. Possibilitar a combinação ou conjugação de duas ou mais tarefas diferentes
- 8.42.55. Deve ser compatível com o software VMS descrito neste termo de referência;
- 8.42.56. Deve possuir garantia mínima de 3 (três) anos;

**8.43. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE CÂMERA IP - TIPO 1, 2, 3 ou 4**

- 8.43.1. Serviço de instalação de câmera IP Tipo 1, 2, 3 ou 4 compreende:
- 8.43.2. Instalação física da câmera IP Tipo 1, 2, 3 ou 4 no ambiente designado, podendo ser em postes, paredes, forros, marquises, conforme planejamento baseado nas plantas baixas fornecidos pela CONTRATANTE;
- 8.43.3. Ajuste de posicionamento, zoom, foco e ângulo da câmera, para que possa ter a melhor visibilidade possível do ambiente a ser monitorado;
- 8.43.4. Conexão da câmera IP Tipo 1, 2, 3 ou 4 na rede de comunicação de dados através de link de dados óptico ou metálico, designado para este fim;
- 8.43.5. Deverá prever a identificação física da câmera IP Tipo 1, 2, 3 ou 4;
- 8.43.6. Serviço de configuração da câmera IP Tipo 1, 2, 3 ou 4 compreende:
- 8.43.7. Configurações básicas da câmera no software VMS, atribuição de nome, atribuição de IP, configurações de imagens, resolução, qualidade de imagem, streamings de vídeo, configurações de armazenamento e configurações gerais;
- 8.43.8. Devem ser instaladas e implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades e a configuração da câmera IP Tipo 1, 2, 3 ou 4, explorando suas características, dentro das melhores práticas de rede, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

**8.44. CÂMERA IP - TIPO 5**

- 8.44.1. Câmera em formato bullet de 2MP com IR 30m e Vídeo Análise, onde deverá possuir no mínimo as seguintes características:
- 8.44.2. Possuir sensor CMOS de 1/2.8" ou maior, com varredura progressiva, com operação Dia/Noite, através de filtro de infra-vermelho mecânico;
- 8.44.3. Deve possibilitar ajuste do ângulo de visualização horizontal pelo menos entre 33° a 104° com lente varifocal de 3.2 a 10mm, com ajustes de lente e foco remotos;
- 8.44.4. Possuir resolução de 2MP pixels ativos em NTSC 16:9 e 9:16 a 30FPS;
- 8.44.5. Caixa de proteção robusta de alumínio extrusado;
- 8.44.6. Suportar áudio bidirecional;
- 8.44.7. Suportar protocolos: IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, Telnet, ARP, DHCP, SNMP (V1, MIB-II), 802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, CHAP, Digest Authentication.
- 8.44.8. Conexão Ethernet 10/100 Base-T, auto-sensing, half/full duplex, com conector RJ45 incorporado na câmera. Não será aceito conversor IP externo. O mesmo deve ser parte integrante da câmera;
- 8.44.9. Suportar operação com compressão H264 e H.265 com qualidade de 2MP a velocidade de 30fps.
- 8.44.10. Deve estar em conformidade com a especificação ONVIF Profile S e T.
- 8.44.11. Deve implementar formato de compressão de vídeo em H.264, H.265 e M-JPEG, e possuir largura de banda configurável em H.265;
- 8.44.12. Deve permitir transmissão simultânea de pelo menos dois streams de vídeo em H265;
- 8.44.13. Suportar iluminação de 30m de alcance com LEDs de 850nm embutidos e de acionamento automático e intensidade ajustável;
- 8.44.14. Alimentação de 12 VDC e PoE (IEEE 802.3af);
- 8.44.15. Suporte obturador de 1/25 a 1/15.000 seg;
- 8.44.16. Deve possuir sensibilidade igual ou melhor a 0,06 lux no modo colorido e no 0,02 lux modo monocromático e 0,0 lux com IR ligado. Estes níveis de sensibilidade devem ser obtidos de acordo com a norma IEC 62676-5 ou similar de mesma capacidade técnica de medição;
- 8.44.17. Possuir WDR real (T-WDR) mínimo de 100dB de acordo com a norma IEC 62676-5 ou similar de mesma capacidade técnica de medição e ainda que

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

comprove a qualidade do processamento de WDR pelo sensor e não por software embarcado na câmera. Não será aceito câmera com WDR processado digitalmente;

- 8.44.18. Fornecer suporte para fixação em parede do mesmo fabricante da câmera;
- 8.44.19. Classificação contra resíduos sólidos e líquidos IP66;
- 8.44.20. Classificação contra impactos IK10, inclusive para o vidro de proteção da lente da câmera.
- 8.44.21. Deve possibilitar operação no range de temperatura de -30°C até 50°C;
- 8.44.22. Deve permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no website do mesmo;
- 8.44.23. A câmera deve possuir botão físico de reset incorporado no hardware da câmera, acessível pelo lado externo da câmera, ou interno, desde que protegido por algum tipo de tampa ou cúpula/domo, sem a necessidade de abertura da caixa da câmera ou que viole o selo de garantia da mesma, evitando-se o contato com o circuito eletrônico interno. O uso do botão de reset deve proporcionar segurança física local para restauração aos padrões de fábrica;
- 8.44.24. Deve possuir recurso integrado de criptografia para o armazenamento em cartão de memória local das imagens;
- 8.44.25. Deve ser fornecido cartão de memória tipo industrial para slot para armazenamento local na câmera do tipo SD/MicroSD card com as seguintes características mínimas:
- 8.44.26. Possuir tecnologia de memória flash MLC NAN com Classe de Velocidade 10, suportando velocidade de leitura de 95MB/s e de gravação de 60MB/s. Deve suportar temperatura de operação de -25°C a +85°C.
- 8.44.27. O cartão de memória deve ser dimensionado para retenção local de imagens e metadados de vídeo análise por período mínimo de 5 dias, na resolução máxima da câmera (2MP), em 5fps e gravação contínua 24h/dia, considerando até 60% do tempo em cena de baixa movimentação (cena estática) e 40% em alta movimentação (alto tráfego, bitrate máximo da câmera).
- 8.44.28. Apresentar juntamente com a documentação de habilitação técnica a memória de cálculo deste armazenamento em ferramenta oficial do fabricante, e garantido na fase de testes e comissionamento;
- 8.44.29. Deve possuir recurso de análise de vídeo embarcada na câmera e possibilitar o uso simultâneo de no mínimo 6 (seis) algoritmos diferentes.
- 8.44.30. Caso a câmera não possua capacidade incorporada de processamento de 6 algoritmos diferentes simultâneos, será aceito sistema de análise de vídeo baseada

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

em servidor externo, desde que o mesmo possua performance suficiente para executar no mínimo 6 (seis) algoritmos simultâneos por câmera 24h/dia, com licenciamento para o total de câmeras com este recurso solicitado.

- 8.44.31. Catálogo e descritivo técnico do sistema baseado em servidor externo deverá ser apresentado juntamente com a documentação de comprovação técnica dos demais itens.
- 8.44.32. Deve ser integrado e homologado pelo fabricante do sistema de gerenciamento de vídeo ofertado.
- 8.44.33. Deve ser baseado em servidor e deve possuir recurso ativo de busca forense nas imagens gravadas e armazenadas com base nos mesmos algoritmos mínimos solicitados.
- 8.44.34. A câmera ou o sistema e software externo de vídeo análise deve possuir disponibilidade para no mínimo os seguintes algoritmos de análise de vídeo:
- 8.44.35. Detectar objetos na área, e/ou entrando, e/ou saindo de uma área
- 8.44.36. Detectar cruzamento de 3 linhas virtuais, combinadas em lógica e/ou;
- 8.44.37. Detectar objetos através de uma rota;
- 8.44.38. Detectar permanência prolongada de pessoa em uma área em função do raio e do tempo;
- 8.44.39. Detectar objetos deixados por um determinado tempo;
- 8.44.40. Detectar objetos removidos;
- 8.44.41. Detectar objetos com determinadas características como: tamanho, velocidade, direção, cor e mudança de relação de aspecto em um tempo determinado (por exemplo, alguém caindo no chão);
- 8.44.42. Contar objetos cruzando uma linha virtual;
- 8.44.43. Contar objetos em uma área e alarmar se um limite pré definido for atingido;
- 8.44.44. Detectar nível de ocupação (multidão) em uma área pré-definida;
- 8.44.45. Possibilitar a combinação ou conjugação de duas ou mais tarefas diferentes;
- 8.44.46. Deve ser compatível com o software VMS descrito neste termo de referência;
- 8.44.47. Deve possuir garantia mínima do fabricante de 3 (três) anos;

**8.45. CÂMERA IP - TIPO 6**

- 8.45.1. Câmera em formato bullet de 2MP e Video Análise, onde deverá possuir no mínimo as seguintes características:
- 8.45.2. Deve possuir sensor de imagem em estado sólido de 1/2.8" ou maior, com

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
varredura progressiva;

- 8.45.3. Deve possuir lente varifocal de no mínimo 2,8 mm a 12 mm;
- 8.45.4. Deve possibilitar ajustes do ângulo de visualização horizontal pelo menos entre 33° e 100°.
- 8.45.5. Deve possuir o recurso de ajuste remoto de zoom e foco;
- 8.45.6. Deve possuir lente tipo: DC-Iris ou P-Iris;
- 8.45.7. Deve possuir filtro de corte de infravermelho removível automaticamente;
- 8.45.8. Deve possuir tempo do obturador entre 1/30s e 1/15000s;
- 8.45.9. Deve possuir capacidade de armazenamento local através de SD/MicroSD card, compact Flash ou USB memory card, onde este deve garantir um período de retenção mínimo de 20 dias, na resolução máxima da câmera, em 10 fps, gravação contínua, com até 50% do tempo em cena de baixa movimentação;
- 8.45.10. O memorial de cálculo deve ser apresentado em ferramenta oficial do fabricante, e garantido na fase de testes e comissionamento;
- 8.45.11. A câmera deve permitir criptografia para as gravações em armazenamento local (SD/MicroSD card, compact Flash ou USB memory card);
- 8.45.12. Deve possuir um criptoprocessador seguro (chip TPM - Trusted Platform Module), capaz de armazenar chaves criptográficas que protejam informações, mesmo em caso de acesso físico à eletrônica (hardware) da câmera, visando um alto nível de segurança da informação;
- 8.45.13. Obs.: Caso a câmera não possua criptoprocessador seguro, deverá ser fornecido sistema IDS (Intrusion Detection System) e IPS (Intrusion Protection System)
- 8.45.14. Deve possuir iluminador infravermelho incorporado com alcance de pelo menos 60m;
- 8.45.15. Classificação contra resíduos sólidos e líquidos IP67;
- 8.45.16. Classificação contra impactos IK10.
- 8.45.17. Deve possuir resolução mínima de 2 Megapixels;
- 8.45.18. Deve suportar relação de aspecto 9:16 em resolução Full HD e HD;
- 8.45.19. Deve permitir a transmissão em resolução 1080p à taxa de frames de 30, com no mínimo 2 fluxo(s) de vídeo configurável(s) de forma independente no codec de compressão mais atual da câmera.
- 8.45.20. Deve possibilitar compensação automática para tomada de imagem contra luz de

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

fundo;

- 8.45.21. Deve possuir Wide Dynamic Range com pelo menos 107dB, em acordo com a IEC 67626 Part 5;
- 8.45.22. Deve possuir sensibilidade mínima igual ou inferior a no modo colorido a 0,0225 lux e 0,0 lux com IR ligado, com FStop de 1.4 e pelo menos 30 IRE;
- 8.45.23. Deve incorporar Balanço de Branco Automático e Manual;
- 8.45.24. Deve suportar valores definidos manualmente para: nível de cor, brilho e contraste;
- 8.45.25. Deve ser fornecida com capacidade embarcada para a configuração de pelo menos 8 máscaras de privacidade na própria câmera;
- 8.45.26. Deve ser equipada com funcionalidade integrada de eventos, que podem ser desencadeados por: detecção de movimento, evento agendado, violação da câmera, acionamento manual;
- 8.45.27. Deve responder a estes eventos através de: Notificações usando HTTP, HTTPS ou email; Envio de imagens por FTP, HTTP, HTTPS ou email; Envio de vídeo clipe por FTP;
- 8.45.28. Deve ser fornecida com capacidade instalada para detectar movimentos;
- 8.45.29. Deve realizar análise de vídeo embarcada, com as seguintes funcionalidades:
- 8.45.30. Detectar objetos estando entrando ou saindo de uma área
- 8.45.31. Detectar cruzamento de até 3 linhas virtuais, combinadas em lógica e/ou;
- 8.45.32. Detectar objetos através de uma rota;
- 8.45.33. Detectar “loitering” em uma área em função do raio e do tempo;
- 8.45.34. Detectar objetos que foram deixados por um determinado tempo;
- 8.45.35. Detectar objetos removidos;
- 8.45.36. Detectar objetos com determinadas características como: tamanho, velocidade, direção, e mudança de relação de aspecto em um tempo determinado (por exemplo, alguém caindo no chão);
- 8.45.37. Contar objetos cruzando uma linha virtual;
- 8.45.38. Contar objetos em uma área e alarmar se um limite pré definido for atingido;
- 8.45.39. Detectar um certo nível de ocupação (multidão) em uma área pré definida;
- 8.45.40. Combinar tarefas usando scripts;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.45.41. Obs.: Caso a câmera não possua os analíticos acima, são aceitos item baseado em servidor, desde que o mesmo possua performance suficiente para executar no mínimo 08 (oito) das tarefas acima de forma simultânea e seja compatível com o sistema de gerenciamento de vídeo ofertada.
- 8.45.42. Deve fornecer níveis de compressão configuráveis;
- 8.45.43. Deve ser fornecida com capacidade embarcada para espelhamento de imagem;
- 8.45.44. Ser capaz de Deve fornecer fluxos H.265, H.264 e Motion JPEG de forma independente e simultânea;
- 8.45.45. Deve possuir funcionalidade de PTZ digital com posições pré-definidas;
- 8.45.46. Deve possuir porta para conexão em rede TCP/IP com conector RJ-45 100BASE-T;
- 8.45.47. Deve possuir largura de banda configurável em H.265 e H.264;
- 8.45.48. Deve possuir os protocolos: RTP, RTSP, UDP, TCP, IPv4, IPv6, DHCP, HTTP, IGMP, SNMP, SMTP, UPnP e DNS;
- 8.45.49. Deve suportar qualidade de serviço (QoS) para ser capaz de priorizar o tráfego;
- 8.45.50. Deve possuir os protocolos de segurança HTTPS e SSL/TLS e seguir o padrão IEEE802.1x de autenticação em rede;
- 8.45.51. Deve estar em conformidade com a especificação ONVIF Profile S.
- 8.45.52. Deve possuir arquitetura aberta para integração com outros sistemas;
- 8.45.53. Deve possuir pelo menos 1 entrada e 1 saída de alarme;
- 8.45.54. Deve possuir entrada e saída de áudio;
- 8.45.55. Deve possuir garantia do fabricante de pelo menos 3 ano(s) comprovada por carta de fabricante e ou informação constante no site do fabricante;
- 8.45.56. Deve possibilitar operação no range de temperatura de -40 °C até 60 °C;
- 8.45.57. Deve possuir aprovações: EN, FCC, VCCI;
- 8.45.58. Deve permitir alimentação PoE conforme padrão IEEE 802.3af (Classe 3) sem uso de equipamentos adicionais;
- 8.45.59. Deve conter um servidor web embutido tornando vídeo e configuração disponíveis para vários clientes em um sistema operacional padrão e ambiente do navegador utilizando HTTP, sem a necessidade de software adicional;
- 8.45.60. Deve permitir atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware no web site do mesmo;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.45.61. Deve possuir botão físico para reset do equipamento;
- 8.45.62. Obs.: Não será aceito conversor IP externo. O mesmo deve ser parte integrante da câmera
- 8.45.63. Deve ser compatível com o software VMS descrito neste termo de referência;
- 8.45.64. Deve possuir garantia mínima do fabricante de 3 (três) anos;

**8.46. CÂMERA IP - TIPO 7**

- 8.46.1. Câmeras em formato dome PTZ de 2MP com IR, IP66 e Vídeo Análise. Câmera móvel para aplicações externas, de alta definição, com o acondicionamento próprio do fabricante do conjunto dome/câmera sem qualquer tipo de adaptação/ alteração ou utilização de módulos de acondicionamento fabricados por terceiros.  
As câmeras PTZ - IP HD deverão possuir no mínimo as seguintes características:
- 8.46.2. Deve possuir sensor de imagem em estado sólido do tipo CMOS de 1/2.8" ou maior, com escaneamento progressivo;
- 8.46.3. Deve possuir lente com zoom ótico de pelo menos 30x com distâncias focais mínimas de 4.5 a 135mm ou superior, com campo de visão horizontal de 24 a 60° Zoom digital mínimo de 16x;
- 8.46.4. Deve possuir resolução HDTV mínima de 1920x1080 pixels a 60 FPS e atender as normas do ONVIF profile S e G (Open Network Video Interface Fórum);
- 8.46.5. Sensibilidade mínima deverá ser igual ou inferior 0,05 lux em modo colorido com IRE30 e velocidade obturador igual ou mais rápida que 1/30s, e 0 lux com iluminador Infravermelho ativo integrado com capacidade para no mínimo 180m;
- 8.46.6. Deve possuir lente com ajuste de foco automático;
- 8.46.7. Deve conter plataforma móvel na câmera com as seguintes características:
- 8.46.8. Deve apresentar, no mínimo, movimento de rotação horizontal ("pan") de 360° (trezentos e sessenta) graus contínuos e movimento de rotação vertical ("tilt") de 0 a 90 (zero a noventa) graus.
- 8.46.9. Velocidade de varredura variável em modo normal:
- 8.46.10. horizontal ("pan") de 1°/s a 240°/s e
- 8.46.11. vertical ("tilt") de 1°/s a 120°/s;
- 8.46.12. Deve possuir sistema de coordenadas atendendo ao padrão WGS 84 (World Geodetic System), que é uma descrição do sistema de coordenadas esféricas do mundo e é utilizado em muitos padrões tal como GPS.
- 8.46.13. Deve implementar formato de compressão de vídeo em H.264, H.265 e M-JPEG

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.46.14. Deve permitir transmissão simultânea de pelo menos dois streams de vídeo em H.264 e H265, sendo:
- 8.46.15. Visualização: resolução 1080p (1920x1080 pixels) em 30 fps;
- 8.46.16. Gravação: resolução 720p (1280x720 pixels) em 10 fps;
- 8.46.17. Deve possibilitar compensação automática para tomada de imagem contra luz de fundo;
- 8.46.18. Deve dispor de, no mínimo, 250 posições pré-programadas (Presets), 1 tour definido pelas pré-posições e 2 tours de ronda programada com duração de 15 minutos no total;
- 8.46.19. Deve possuir zonas de mascaramento de imagem programáveis embarcada na câmera e que possa inserir, no mínimo, 24 máscaras de privacidade com configuração individual e 16 setores independentes com identificação;
- 8.46.20. Possuir recurso de criação de no mínimo 8 alarmes simultâneos em até 16 áreas distintas e poligonais para associação aos alarmes.
- 8.46.21. Possuir função FLIP para girar automaticamente a câmera em 180° quando estiver seguindo um alvo que se movimenta imediatamente por baixo da câmara.
- 8.46.22. Possuir WDR real (T-WDR) mínimo de 94dB de acordo com a norma IEC 62676-5 ou 120dB Forense. Não será aceito câmera com WDR processado digitalmente, ou seja, D-WDR.
- 8.46.23. Conexão Ethernet 10/100 Base-T, auto-sensing, half/full duplex, com conector RJ45 incorporado na câmera. Não será aceito conversor IP externo, o mesmo deve ser parte integrante da câmera;
- 8.46.24. Deve possuir protocolos Internet: RTP, UDP, TCP, IPv4, IPv6, HTTP, IGMP, SNMP (V1, V3, MIB-II), SMTP e DNS;
- 8.46.25. Deve possuir os protocolos de segurança HTTPS e IEEE802.1x;
- 8.46.26. A câmera deve permitir alimentação através do cabo de rede PoE+ (High Power Over Ethernet) com padrão IEEE 802.3at ou superior, sem uso de equipamentos externos adicionais;
- 8.46.27. Deve operar simultaneamente alimentação PoE+ com alimentação externa 24VAC de forma a garantir alimentação redundante à câmera;
- 8.46.28. Deve possuir a possibilidade de atualização de software e firmware através de software do fabricante da câmera, com disponibilização das versões de firmware na web site do mesmo;
- 8.46.29. A câmera deve possuir botão físico de reset incorporado no hardware da câmera, acessível pelo lado externo da câmera, ou interno, desde que protegido por algum tipo de tampa ou cúpula/domo, sem a necessidade de abertura da caixa da câmera

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

ou que viole o selo de garantia da mesma, evitando-se o contato com o circuito eletrônico interno. O uso do botão de reset deve proporcionar segurança física local para restauração aos padrões de fábrica;

- 8.46.30. Deve permitir o acesso simultâneo de, no mínimo, 4 usuários em unicast e suportar o protocolo IGMP (multicast);
- 8.46.31. Deve suportar protocolo QoS (Qualidade de Serviço) para ser capaz de priorizar o tráfego;
- 8.46.32. Especificação da integração com outros sistemas
- 8.46.33. Deve possuir arquitetura aberta para integração com outros sistemas;
- 8.46.34. Deve conter caixa de proteção pendente em alumínio que deve proteger totalmente a câmera de chuva, poeira, umidade e uso externo com grau de proteção IP66. A caixa de proteção, bem como seus acessórios, deverá ser do mesmo fabricante da câmera ou homologado pela mesmo garantindo a qualidade do conjunto;
- 8.46.35. Deve possuir caixa de proteção com capacidade de trabalhar com temperatura até +60°C e umidade de até 90%, sem causar danos a câmera;
- 8.46.36. Deve possuir braço de fixação em postes do mesmo fabricante com entradas pré-perfuradas para os cabos de comunicação;
- 8.46.37. Deve possuir caixa externa vedada, do próprio fabricante, para junção do braço de fixação da câmera ao poste. Todos os acessórios adicionais devem ser previstos para que a seja feita a fixação da câmera ao poste;
- 8.46.38. Possuir duas entradas de alarme e uma saída de relê;
- 8.46.39. Possuir uma interface para conexão de áudio bidirecional;
- 8.46.40. Compatibilidade Eletromagnética (EMC) de acordo com FCC Parte 15 e CE;
- 8.46.41. Segurança do Produto de acordo com regulamentos CE, UL, e padrões da IEC.
- 8.46.42. Deve apresentar documento que comprove MTBF (Tempo Médio Entre Falhas) de no mínimo 100.000 horas.
- 8.46.43. Deve possuir slot para armazenamento local em cartão de memória do tipo SD ou MicroSD card compact Flash, com capacidade mínima de armazenamento de 256GB.
- 8.46.44. Deve possuir recurso integrado de criptografia para o armazenamento em cartão de memória local das imagens
- 8.46.45. Deve ser fornecido cartão de memória tipo industrial para slot para armazenamento local na câmera do tipo SD/MicroSD card com as seguintes características mínimas:

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.46.46. Possuir tecnologia de memória flash MLC NAN com Classe de Velocidade 10, suportando velocidade de leitura de 95MB/s e de gravação de 60MB/s. Deve suportar temperatura de operação de -25° a +85°C;
- 8.46.47. O cartão de memória deve ser dimensionado para retenção local de imagens por período mínimo de 10 dias, na resolução máxima da câmera (2MP), em 10fps e gravação contínua (24h), considerando até 50% do tempo em cena de baixa movimentação (cena estática) e 50% em alta movimentação (alto tráfego, bitrate máximo da câmera);
- 8.46.48. Apresentar juntamente com a documentação de habilitação técnica a memória de cálculo deste armazenamento em ferramenta oficial do fabricante, e garantido na fase de testes e comissionamento
- 8.46.49. Deve possuir recurso de análise de vídeo embarcada na câmera ou em servidor de vídeo análise e possibilitar o uso simultâneo de no mínimo 6 (seis) algoritmos diferentes por câmera para pelo menos 12 presets;
- 8.46.50. Caso a câmera não possua capacidade de análise de vídeo incorporada, será aceito item com análise de vídeo baseada em servidor externo, desde que o mesmo possua performance suficiente para executar no mínimo 6 (seis) algoritmos simultâneos por câmera, com licenciamento para o total de câmeras com este recurso solicitado. Catálogo e descritivo técnico do item proposto baseado em servidor externo deverá ser apresentado juntamente com a documentação de comprovação técnica. O item proposto deve ser integrado e homologado pelo fabricante do sistema de gerenciamento de vídeo ofertado.
- 8.46.51. Deve possuir recurso ativo de BUSCA FORENSE com base nas imagens gravadas em storage e/ou no cartão de memória da câmera, possibilitando busca de alarmes baseados nos metadados dos mesmos algoritmos mínimos solicitados.
- 8.46.52. Deve possuir disponibilidade para no mínimo os seguintes algoritmos de análise de vídeo:
- 8.46.53. Detectar objetos na área, entrando na área, ou saindo da área demarcada
- 8.46.54. Detectar cruzamento de 1 a 3 linhas virtuais, combinadas em lógica e/ou;
- 8.46.55. Detectar objetos através de uma rota;
- 8.46.56. Detectar permanência prolongada de pessoa em uma área em função do raio e do tempo;
- 8.46.57. Detectar objetos deixados por um determinado tempo;
- 8.46.58. Detectar objetos removidos;
- 8.46.59. Detectar objetos com determinadas características como: tamanho, velocidade, direção, cor e mudança de relação de aspecto em um tempo determinado (por exemplo, alguém caindo no chão com roupa de cor predominante azul);

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.46.60. Contar objetos cruzando uma linha virtual;
- 8.46.61. Contar objetos em uma área e alarmar se um limite pré definido for atingido;
- 8.46.62. Detectar nível de ocupação (multidão) em uma área pré-definida;
- 8.46.63. Possibilitar a combinação de duas ou mais tarefas de vídeo análise simultâneas;
- 8.46.64. Deve ser compatível com o software VMS descrito neste termo de referência;
- 8.46.65. Deve possuir garantia mínima de 3 (três) anos;

**8.47. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE CÂMERA IP - TIPO 5, 6 ou 7**

- 8.47.1. Serviço de instalação de câmera IP Tipo 5, 6 ou 7 compreende:
- 8.47.2. Instalação física da câmera IP Tipo 5, 6 ou 7 no ambiente designado, podendo ser em postes, paredes, forros, marquises conforme planejamento baseado nas plantas baixas fornecidos pela CONTRATANTE;
- 8.47.3. Ajuste de posicionamento, zoom, foco e ângulo da câmera, para que possa ter a melhor visibilidade possível do ambiente a ser monitorado;
- 8.47.4. Conexão da câmera IP Tipo 5, 6 ou 7 na rede de comunicação de dados através de link de dados óptico ou metálico, designado para este fim;
- 8.47.5. Deverá prever a identificação física da câmera IP Tipo 5, 6 ou 7;
- 8.47.6. Serviço de configuração da câmera IP Tipo 5, 6 ou 7 compreende:
- 8.47.7. Configurações básicas da câmera no software VMS, atribuição de nome, atribuição de IP, configurações de imagens, resolução, qualidade de imagem, streamings de vídeo, configurações de armazenamento e configurações gerais;
- 8.47.8. Devem ser instaladas e implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades e a configuração da câmera IP Tipo 5, 6 ou 7, explorando suas características, dentro das melhores práticas de rede, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação.

**8.48. SOLUÇÃO DE GERENCIAMENTO DE VIDEOMONITORAMENTO VMS**

- 8.48.1. A Solução de gerenciamento de videomonitoramento VMS deve conter no mínimo as seguintes características:
- 8.48.2. Solução de sistema de vídeo segurança deve ser integrado, multiusuário e multi-site. Deve suportar um número ilimitado de servidor de gravação e visualização de câmeras IP, codificadores de vídeo IP;
- 8.48.3. Gerenciamento otimizado de armazenamento de vídeo: A solução deve dispor de arquivamento único, gravação de longa duração de bom desempenho, escalabilidade e custo-eficiente;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.48.4. Detecção automática de modelo de câmera: Deve suportar mais de 10000 modelos de câmeras IP, codificadores de vídeo IP, e mais de 150 fornecedores diferentes, utilizando métodos como a Universal Plug and Play, Broadcast, varredura manual e varredura por faixa de IP;
- 8.48.5. Número ilimitado de servidores de gravação: Deve suporta um número ilimitados de câmeras por servidor. Gravação continua ou ativada por movimento, evento ou agendamento;
- 8.48.6. Rede e armazenamento otimizados: Deve suportar multi-streaming que otimiza a banda usando novos métodos de compressão; MPEG4, H.264, H.265 além MJPEG e MPEG4;
- 8.48.7. Deve suportar a utilização de múltiplos fluxos de vídeo de cada câmera para ao visualização e gravação com diferentes configurações de modo a otimizar largura de banda e armazenamento;
- 8.48.8. Deve ser capaz de armazenar conteúdo em vídeo que não são críticos em diferentes topologias e arquitetura de armazenamento;
- 8.48.9. Deve suportar a detecção de movimento, independente do modelo da câmera; seja pelo servidor ou pela camera; ou simultaneamente;
- 8.48.10. Deve ter capacidade de trabalhar com múltiplos sites independentes através da federação dos mesmos em um único site central, garantindo o monitoramento e gestão dos dispositivos de forma unificada. A plataforma/Licença que interconecta sistemas remotos/menores ao site central permitindo um número ilimitado de dispositivos conectados a um sistema central
- 8.48.11. Deve suportar comunicação criptografada entre todos os elementos do sistema com chaves geradas por entidades certificadas externas.
- 8.48.12. Plataforma Aberta: Deve fornecer API / SDK de forma gratuita e suportar integração com hardware ou aplicativos de terceiros.
- 8.48.13. Integração nativa de todos os dispositivos compatíveis com os fóruns de compatibilidade Onvif Profile S, Q e T e PSIA.
- 8.48.14. Instalação em Windows 64 bits
- 8.48.15. Compatível com Instalações em ambiente virtualizado VMWare e Microsoft Hyper-V
- 8.48.16. Deve permitir exibição do alerta gerado pelos dispositivos, através do processamento dos metadados recebido das câmeras / encoders, mostrando os quadros (overlay) nos formatos e cores gerados pelos dispositivos. Tudo isto deve ser permitido através do dispositivo integrado via ONVIF.
- 8.48.17. Deve permitir a integração de sistemas de controle de acesso de forma bi-direcional sem a necessidade de interfaces físicas para tal. Deve permitir que alarmes do sistema de acesso sejam visto na interface do usuário do Sistema de Vídeo assim como o vídeo e os alarmes do mesmo sejam vistos na interface do Sistema de Acesso.
- 8.48.18. Permitir integração com Solução de Vídeo Wall com número ilimitado de monitores;
- 8.48.19. Deve possibilitar total compatibilidade com, no mínimo, duas versões anteriores do sistema;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.48.20. O sistema deve conter os componentes a seguir
- 8.48.21. Serviço de Administração
- 8.48.22. Gerenciamento centralizado: O software de administração deve oferecer um acesso único e consolidado para configuração dos servidores de gravação, mesmo em instalações multisites;
- 8.48.23. Assistentes de configuração: Guia o usuário através do processo de adição de câmeras, a configuração de vídeo e gravação, ajuste de detecção de movimento e configuração do usuário;
- 8.48.24. Detecção automática de dispositivos: permite a detecção rápida de dispositivos e câmeras usando métodos como a Universal Plug and Play, Broadcast e varredura por faixa de IP;
- 8.48.25. Opção de configuração em massa: Altera as configurações em vários dispositivos ao mesmo tempo com poucos cliques; independentemente de estarem no mesmo site ou em sites remotos;
- 8.48.26. Gerenciamento de senhas dos dispositivos diretamente na interface do software. O sistema deve permitir automação de troca periódica das senhas dos dispositivos.
- 8.48.27. Importação de dados de configuração off-line: Permite a edição off-line de dados de configuração, incluindo câmeras e as definições de dispositivos;
- 8.48.28. Sistema automático de pontos de restauração: um ponto de restauração é criado a cada vez que uma mudança de configuração é feita. Permite a reversão fácil de pontos de configuração previamente definidos e permite o cancelamento de mudanças de configuração indesejados e a restauração de configurações anteriores válidas;
- 8.48.29. Deve permitir a personalização da interface de administração de acordo com os direitos de cada usuário, concedendo permissões, restringindo funções e ocultando desabilitando partes da interface para evitar o acesso indevido a ações restritas.
- 8.48.30. Deve permitir a atualização de firmware de câmeras diretamente da interface do VMS . Deve permitir atualização por câmera individualmente ou por grupo de câmeras do mesmo fabricante.
- 8.48.31. Ser nativamente compatível com Microsoft Active Directory para gestão de usuários e perfis de acesso do Windows e permitir autenticação de usuário única (SSO)
- 8.48.32. Permitir controle de acesso aos perfis de usuários: Visualização ao vivo, controle PTZ, presets PTZ, controle de saídas, Eventos, ouça o microfone, fale com a caixa de som remota, gravação manual; Reprodução, exportação AVI, exportação JPG, exportação de banco de dados, sequências, pesquisa inteligente e áudio. Bem como definir as vistas, editar vistas particulares e públicas.
- 8.48.33. Trabalhar com banco de dados centralizado de fabricantes reconhecidos de mercado como SQL Server, Oracle ou MySQL
- 8.48.34. Deve permitir acesso remoto para o software de visualização e aplicativo para visualização em web browsers, com opção de conexão segura no acesso à câmera (HTTPS)
- 8.48.35. Ter servidor de Web embutido para download de softwares e plug-ins.
- 8.48.36. Ter histórico de provas exportadas por usuário e arquivo.
- 8.48.37. Ter histórico de atividade do usuário do cliente pelo tempo, localidade e câmeras.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.48.38. Pode ser instalado em conjunto com o servidor de gravação.
- 8.48.39. Fornecer streams múltiplos de vídeo ao vivo para diferentes clientes.
- 8.48.40. Serviço de Servidor Móvel
- 8.48.41. O sistema deve suportar:
- 8.48.42. Acesso remoto para clientes móveis.
- 8.48.43. Realiza o login e solicitações de acesso entre clientes e o Servidor Master.
- 8.48.44. Redimensiona as imagens de vídeo vigilância para ajustar ao layout da tela dos dispositivos móveis.
- 8.48.45. Pode ser instalado em conjunto do servidor de gravação.
- 8.48.46. Deve permitir ser instalado em dispositivos com sistema operacional iOS, Android e Windows Phone
- 8.48.47. Deve permitir a transmissão de imagens geradas em tempo real pela câmera do dispositivo móvel para a central de monitoramento, e gravar estas imagens no sistema como se fosse um dispositivo fixo já instalado no sistema.
- 8.48.48. Deve permitir a Inclusão do geo posicionamento através de meta dados de GPS advindos do dispositivo móvel.
- 8.48.49. Deve permitir eventos/alarmes no dispositivo móvel em tempo real;
- 8.48.50. Serviço de Gestão de Eventos e Alarmes
- 8.48.51. Deve ter um motor (engine) que forneça regras para a automação de diferentes aspectos do sistema, incluindo controle da câmera, comportamento do sistema e dispositivos externos, com base em eventos ou horários.
- 8.48.52. Deve fornecer uma caixa de diálogo de configuração no estilo Microsoft Outlook, na qual eventos predefinidos e personalizados são usados nas regras para acionar ações.
- 8.48.53. Teve ter as seguintes categorias de eventos:
- Hardware: dispositivos de hardware físico conectados ao sistema.
  - Dispositivos: certas funções e estados de dispositivos disponíveis através de dispositivos de hardware conectados.
  - Externo: relacionado às integrações do VMS.
  - Servidor de gravação: funções de arquivamento e banco de dados.
  - Análise: a partir de aplicativos e sistemas de análise integrados.
  - Definido pelo usuário: Eventos configurados de forma personalizada, permitindo que os usuários disparem
  - Perfis de horário.
- 8.48.54. Ter gerenciamento de evento / alarme de ponto único: gerenciamento central de todos os alarmes internos do sistema e alarmes externos de segurança.
- 8.48.55. Ter suporte à associação de alarmes a mapas.
- 8.48.56. Deve possuir um Gerenciador de Alarmes que permita:

Lista de alarmes com amplos recursos de classificação e filtragem.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Visualização instantânea de vídeo gravado de câmeras primárias e relacionadas, no momento do incidente.

Imagem em miniatura da câmera principal, no momento do incidente.

A opção de desativação de alarme deve permitir que os usuários suprimam alarmes de um determinado dispositivo por um período de tempo especificado.

- 8.48.56.1. e Relatórios de tratamento de alarmes, fornecendo informações sobre a entrada e o desempenho do tratamento de alarmes.
- 8.48.57. Serviço de Gravação e gerenciamento das gravações
- 8.48.58. O sistema deve suportar:
- 8.48.59. Gravação digital simultânea de vários canais de vídeo e áudio.
- 8.48.60. Transmissão de áudio bidirecional do microfone do cliente para alto-falantes remotos.
- 8.48.61. A otimização da largura de banda devido ao multi-streaming, dividindo o fluxo de vídeo da câmera para fluxos diferenciados para ver vídeo ao vivo e gravado.
- 8.48.62. O software client pode solicitar a visualização ao vivo em uma taxa de quadros diferentes e em resolução mais baixa que as configurações de gravação.
- 8.48.63. Conectividade para as câmeras, codificadores de vídeo e DVRs suportando compressões como MJPEG, MPEG4, MPEG4 ASP, H.264 e MxPEG, H.265.
- 8.48.64. Detecta automaticamente os modelos de câmeras durante a instalação.
- 8.48.65. Número ilimitado de câmeras instaladas.
- 8.48.66. Tecnologia de gravação: banco de dados seguro de alta velocidade de imagens JPEG ou fluxos MPEG4 e H264 incluindo áudio.
- 8.48.67. Velocidade de gravação: Mais de 30 frames por segundo por câmera, limitado apenas pelo hardware e rede.
- 8.48.68. A qualidade da gravação depende inteiramente da câmera e do encoder: não há limitação de software.
- 8.48.69. Capacidade de gravação ilimitada, dependendo apenas da capacidade de storage.
- 8.48.70. Exportação de vídeo configurável por hora ou diária, com passagem automática opcional para unidade de rede de maior capacidade de armazenamento, com imagens disponíveis para reprodução de forma transparente para o operador.
- 8.48.71. Detecção de movimento embutida, em tempo real, com sensibilidade completamente ajustáveis e com zonas de exclusão. Permitindo ativar a gravação com velocidade de frames superior quando é detectado movimento ou quando surge um evento, notificando o alerta por e-mail.
- 8.48.72. Gravação manual com início do tempo baseada em critérios pré-definidos e privilégios de acesso.
- 8.48.73. Pan Tilt Zoom (PTZ) com presets armazenados pelo sistema, sendo em até 50 por câmera.
- 8.48.74. Ativação de presets e patterns quando acontecem determinados eventos.
- 8.48.75. Programação para ativação do pattern em períodos diferentes: isto é, diferente para

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

dia e noite / semana, etc.

- 8.48.76. Varredura PTZ em dispositivos suportados: visualização ou gravação enquanto se move lentamente a partir de uma posição para outra.
- 8.48.77. Acione o limpador ou esguicho de água remotamente, nos modelos suportados de PTZ
- 8.48.78. Em eventos pré-definidos comandos são enviados automaticamente para exibir vídeo ao vivo em computadores remotos.
- 8.48.79. O servidor de gravação é executado como um serviço do Windows.
- 8.48.80. Gravação em multi estágios, permite configurar o sistema para gravar em locais, tempo e taxa de frames diferentes. Permitindo até a redução da taxa de frames automática para atender a demanda de tempo de configuração.
- 8.48.81. Recuperação configurável de trechos de vídeo perdidos diretamente da câmera que possui a função de gravação local (seja através de cartão de memória removível ou memória fixa embutida na câmera).
- 8.48.82. Deve suportar gravação embarcada na câmera (edge storage) em vários fabricantes e em dispositivos ONVIF nos perfis acima mencionados;
- 8.48.83. Serviços de conexão remota aos servidores de imagem.
- 8.48.84. Permitir federação de sistemas independentes do mesmo fabricante, sincronizando a informação de alarmes, usuários, câmeras e gravadores com um sistema central.
- 8.48.85. Permitir a interconexão de câmeras vindas de sistemas independentes (do mesmo fabricante) para um sistema central, trazendo vídeo ao vivo e gravado e seus alarmes associados.
- 8.48.86. Suportar sistemas servidores de gravação de 64 bits, em hardware e software.
- 8.48.87. Assinatura digital no banco de dados garantindo integridade do vídeo.
- 8.48.88. Monitoramento do sistema e do servidor de imagens com relatório das configurações.
  - 8.48.88.1. Redundância da gravação de vídeo. O sistema deve permitir que em caso de falha na gravação dos vídeos, outro assuma, sem a adição de licença para essa função.
- 8.48.89. A redundância poderá ser efetuada em um ou vários (N:N) storage exclusivos para essa função, ou pode ser feito nos mesmos gravadores do sistema.
- 8.48.90. Deve possibilitar mover dispositivos (câmeras ou grupo de câmeras) entre diferentes servidores de gravação;
- 8.48.91. Deve mover todos os dispositivos associados;
- 8.48.92. Deve dispensar reconfiguração de câmeras.
- 8.48.93. Obs.: O serviço de gravação nos servidores de gravação não deve depender da instalação de um banco de dados local para garantir seu funcionamento.
- 8.48.94. Software De Visualização De Gravação
- 8.48.95. Operação
- 8.48.96. O sistema deve suportar:
  - 8.48.97. Visualização ao vivo e reprodução: Clients desde dispositivos móveis a computadores com suporte para visualizar até 100 câmeras de vários servidores ao mesmo tempo.
- 8.48.98. Exibições de Janelas/Layouts: Trabalha com exibições contendo até 10x10

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

câmeras, Hot spot, Matriz, Sequencial, imagens estáticas e ativas, vídeos ao vivo ou gravados, mapas HTML, distribuídos em todos os monitores do computador.

- 8.48.99. Mapas : Os serviços suportados devem incluir serviços de mapas do Bing, Google e OpenStreetMap. Mapas GIS georreferenciados, como shapefiles, desenhos CAD georreferenciados e construção de mapas com vários níveis de piso, com arquivos tipo dwg e dxf.
- 8.48.100. Serviço de Mapa OpenStreetMap Off-line: Suporta o uso do servidor OpenStreetMap fornecido pelo proprietário para uso off-line
- 8.48.101. PTZ inteligente: controle manual, presets, macros (vá à preset quando evento), patrulhamento com esquemas múltiplos (pattern), comandos para limpador (palheta) e esguicho de água, controle por joystick e teclado/mouse.
- 8.48.102. Matriz Virtual: exibições de controle de câmara ao vivo em computadores remotos para visualização distribuída.
- 8.48.103. Controle de Entradas/ Saídas de Alarme: Das câmeras ou dispositivos de I/O, de forma a criar botões/eventos manuais, ou receber sinais de sistemas de intrusão ou controle de acesso.
- 8.48.104. Áudio multicanal bidirecional: Ouça áudio ao vivo/gravado com reprodução instantânea no PC cliente e transmita voz pelo microfone a alto-falantes remotos.
- 8.48.105. Permite gravação de áudio sincronizada a qualquer canal de vídeo.
- 8.48.106. Gravação manual: Baseado em privilégios de acesso definido pelo administrador, os usuários clientes podem manualmente iniciar a gravação de uma câmera por um tempo predefinido.
- 8.48.106.1. Dupla autenticação, exigindo com que o usuário tenha autenticação de um usuário supervisor para conseguir se autenticar no software, protegendo o sistema de acessos indevidos.
- 8.48.107. Stream de visualização adaptativo, onde a resolução da câmera é alterada automaticamente quando o operador muda a visualização do modo mosaico para modo único em tela cheia.
- 8.48.108. Capacidade de enviar vídeos ao vivo e gravado para monitores de vídeo wall dentro da própria interface.
- 8.48.109. Busca, backup e dados seguros
- 8.48.110. O sistema deve suportar:
- 8.48.111. Processamento de gravação: Através da busca de movimento acima do vídeo gravado, PTZ digital com suavização de imagem opcional (apenas no software visualizador).
- 8.48.112. Backup de Evidência: JPEG, AVI, WAV e formatos de dados nativos com software visualizador stand-alone, criptografia de dados e registros, notas de usuários e impressão de relatórios.
- 8.48.113. Autenticação: contas de usuário do Microsoft Active Directory e nativos.
- 8.48.114. Autorização: contas de usuário e grupos do Microsoft Active Directory e perfis de usuário nativos (do sistema), todos os privilégios de acesso e controle de ações permitidas no nível da câmera.
- 8.48.115. Histórico: Todas as ações do usuário por tempo, localizações e câmeras, e toda

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

a operação do sistema.

- 8.48.116. Alerta: Notifica os usuários em caso de detecção de movimento ou evento por som, e-mail ou SMS.
- 8.48.117. O sistema deve suportar:
- 8.48.118. Reprodução de gravações de vídeo e áudio localmente no servidor de gravação.
- 8.48.119. Visualização de até 16 câmeras com tempo sincronizado durante a reprodução.
- 8.48.120. Pesquisa instantânea em gravações com base na data / hora e atividade.
- 8.48.121. Pesquisa inteligente unificada, através de detecção de movimento, marcadores(bookmarks), eventos e alarmes.
- 8.48.122. Pesquisa Forense por metadados: A pesquisa deve poder utilizar eventos de metadados gerados pelas câmeras como ferramenta de busca de imagens.
- 8.48.123. Linha de tempo de atividade com recurso de lupa; possibilitando ampliar ou reduzir a faixa de tempo necessária para dar início a busca por vídeos gravados;
- 8.48.124. Pesquisa instantânea em gravações com base na data / hora e atividade / alarme (Video Motion Detection).
- 8.48.125. Provas podem ser geradas com relatório impresso, imagem em JPEG, AVI ou no formato proprietário (com visualizador incluso), ou ainda pode exportar vídeo em formato MKV padrão.
- 8.48.126. Exportação de gravações de áudio em formato WAV ou AVI.
- 8.48.127. Exportação de vídeo digital com zoom para visualizar área de interesse, e para minimizar o tamanho do arquivo exportado.
- 8.48.128. Criptografia e opção de senha de proteção para as gravações e os arquivos exportados.
  - 8.48.128.1. Capacidade de adicionar comentários às provas exportadas, também criptografadas.
- 8.48.129. Possuir interface proprietária, desenvolvida pelo mesmo fabricante e com mesmo código fonte do servidor de gerenciamento e gravação.
- 8.48.130. Possuir mesma comunicação/ conceito visual do server side.
- 8.48.131. Não possuir banco de dados proprietário local no cliente, devendo qualquer informação inerente ao sistema ser armazenada somente no banco de dados do servidor de gerenciamento/ banco de dados SQL Server.
- 8.48.132. Opção para enviar imagens por e-mail.
- 8.48.133. Aplicativo de visualização através do Web Browser
- 8.48.134. O sistema deve suportar:
- 8.48.135. Visualização de vídeo ao vivo ou reprodução de gravações para 1 a 16 câmeras simultaneamente, advindos do mesmo ou diferentes servidores.
- 8.48.136. Navegação de vídeo avançadas, incluindo reprodução lenta/rápida, salto a data/hora e pesquisa de movimento no vídeo.
- 8.48.137. Exibições individuais podem ser definidas pelo usuário em vários layouts: exibição ou reprodução de imagens da câmera de vários servidores simultaneamente na mesma vista.
- 8.48.138. Vistas compartilhadas podem ser geridas centralmente, através do servidor com permissão de administrador.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.48.139. Importação de mapas estáticos ou ativos para navegação rápida entre câmeras.
- 8.48.140. Controle do relé de saída de alarme.
- 8.48.141. Visão geral das sequências com movimento detectado e janela de visualização.
- 8.48.142. Visão geral de eventos / alertas.
- 8.48.143. Controle de câmeras PTZ remotamente, usando também posições pré-determinadas.
- 8.48.144. Controle remoto de PTZ por clique em ponto.
- 8.48.145. Controle remoto de zoom sinalando um retângulo.
- 8.48.146. Assumir controle manual sobre uma câmara PTZ que executa um esquema de patrulhamento; após um período de tempo sem atividade a câmera volta ao seu patrulhamento programado.
- 8.48.147. Criar arquivos AVI ou criar imagens JPEG geradas a partir de conteúdo gerado pelo software, seja estas imagens advindas de vídeo ou não;
- 8.48.148. Imprimir relatórios de incidentes com os comentários livres e pertinentes ao usuário.
- 8.48.148.1. Sistema de login usando nomes de usuário e senhas cadastrados no sistema proprietário ou delegado ao Microsoft Active Directory.
- 8.48.149. Matriz de Vídeo
- 8.48.150. O sistema deve suportar:
- 8.48.151. Matriz virtual mostrando o vídeo ao vivo diretamente de no mínimo 04 câmeras por cada tela individual a serem acionadas remotamente por comandos remotos e manuais;
- 8.48.152. Seqüência de câmeras tipo FIFO (first-in-first-out)
- 8.48.153. Vários eventos podem controlar um monitor de matriz e eventos únicos pode controlar vários monitores.
- 8.48.154. Visualizar o vídeo na sua taxa máxima de frames em qualquer codec provido pela câmera.
- 8.48.155. Cliente celular
- 8.48.156. O sistema deve suportar:
- 8.48.157. Aplicativos gratuitos para dispositivos baseados em sistema operacional Android (Google), iOS (Apple) e Windows Phone 8
- 8.48.158. Permitir a visualização de múltiplas imagens simultaneamente.
- 8.48.159. Busca e reprodução de vídeo gravado.
- 8.48.160. Toque na tela do dispositivo para zoom digital e diferentes modos de visualização da imagem.
- 8.48.161. Controle das funcionalidades PTZ das câmeras.
- 8.48.162. Salvar ou compartilhar uma foto do vídeo exibido ao vivo.
- 8.48.163. Permitir a utilização da câmera de vídeo do dispositivo móvel como um gerador de imagens para o sistema principal.
- 8.48.164. Opções de Integração
- 8.48.165. O sistema deve ser:
- 8.48.166. Compatível com software de integração de vídeo-vigilância com sistemas ATM ou POS (registro de fluxo de produtos/ pessoas para a gestão de prevenção de perdas e fraudes);
- 8.48.167. Compatível com software supervisorio de alarmes e estado de dispositivos para

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

grandes instalações.

- 8.48.168. Integrado com sistemas de controle de acesso, alarmes, portões, sistemas de gestão, ótica usando os eventos de I/O, eventos internos, eventos TCP/IP ou por OPC DA.
- 8.48.169. Ter SDK gratuito para integração do vídeo em outros produtos usando a API para exibir imagens ao vivo, reprodução de atividades gravadas, mostrar imagens de determinado período de tempo, e buscar por movimento.
- 8.48.170. Criar, importação e usar páginas HTML para a navegação entre os pontos de vista ou para ativar a matriz virtual no software de visualização.
- 8.48.171. Integrado nativamente com todos os dispositivos listados nos fóruns de compatibilidade Onvif, Profile S e PSIA.
- 8.48.172. Licenciamento
- 8.48.173. Deve estar composto por:
  - 8.48.174. Licença de Sistema
  - 8.48.175. Obrigatório para a instalação do produto
  - 8.48.175.1. Deve abranger a instalação de um número ilimitado de servidores usando a mesma licença do software de código e a designação de servidores.
- 8.48.176. A licença contempla um número ilimitado de servidores de gravação, softwares clientes, clientes web e aplicativos móveis.
- 8.48.177. Não tem validade e ser de propriedade do contratante.
- 8.48.178. Todos os softwares clientes não deverão ser licenciados e podem ser instalados e utilizados em qualquer número de computadores, de forma gratuita.
- 8.48.179. Acordo de Manutenção do Produto: Esta licença garante a aquisição e uso de forma gratuita de todas as atualizações dos produtos. Deverá ser adquirida para 3 anos.
- 8.48.180. Expansão Do Sistema
- 8.48.181. A expansão do sistema não deve ser atrelada a quantidade atual de servidores / câmeras.
- 8.48.182. O número de servidores de gravação deve permitir ser ampliado a qualquer momento, sem necessidade de licenciamento adicional, seja local ou remoto.
- 8.48.183. O número de câmeras pode ser ampliado independente da quantidade de servidores de gravação e/ou estações de operação do sistema.
- 8.48.184. O número de clientes de operação e de dispositivos móveis, poderá ser ampliado a qualquer momento sem necessidade de licenciamento adicional.

**8.49. LICENÇA GERENCIAMENTO DE VIDEOMONITORAMENTO POR CANAL IP**

- 8.49.1. Licença compatível com o software VMS descrito nesta especificação, que atendam todas suas características e funcionalidades;
- 8.49.2. Deve ser capaz de ativar 1 (um) canal de câmera IP;

**8.50. LICENÇA GERENCIAMENTO DE VIDEOMONITORAMENTO SUPORTE LPR**

- 8.50.1. A licença para gerenciamento de videomonitoramento para LPR deve possuir as

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

seguintes características mínimas:

- 8.50.2. Sistema de Leitura de matrícula/placa deve ser do mesmo desenvolvedor da solução de gerenciamento de videomonitoramento VMS descritos nesta especificação técnica para uma melhor integração e funcionamento
- 8.50.3. Deve comparar lista de placas previamente configuradas com as imagens ao vivo capturadas por câmeras de vídeo monitoramento IP homologadas pelo fabricante de software.
- 8.50.4. Deve possuir reconhecimento de placas de mais de 100 países e estados em todo mundo
- 8.50.5. Deve atrelar captura de placa a uma regra de captura e registro de vídeo capturando todo trajeto e captura.
- 8.50.6. Criação de listas permitidas, negadas e captura automática de todas placas.
- 8.50.7. Deve apresentar captura ao vivo acompanhado do vídeo também capturado ao vivo
- 8.50.8. Deve possuir módulos de placas para diversos países
- 8.50.9. Deve ser atrelado ao sistema de vídeo monitoramento de software dando capacidade de criação de regras, eventos e alarmes.
- 8.50.10. Deve possuir funcionalidades de compensação de distorção de vídeo e posição incorreta de placas capturadas de um veículo;
- 8.50.11. Deve ser capaz de armazenar uma sequência de vídeo completa associado ao resultado de reconhecimento de placas;
- 8.50.12. Deve suportar o reconhecimento de placas de todo território nacional;
- 8.50.13. Deve fornecer ajuste de parâmetros de reconhecimento e grau de confiança;
- 8.50.14. Deve ter a capacidade de gerenciamento remoto;
- 8.50.15. Deve suportar listas internas das placas registradas (Branca, Negra e Informativa);
- 8.50.16. Deve fornecer interface flexível ao operador para resolução de diferentes tarefas;
- 8.50.17. Deve fornecer diversos métodos de pesquisa, seja por placa capturada, data e/ou horário e resultados associados com imagens/vídeo das placas;
- 8.50.18. Deve ser capaz de pesquisar por qualquer sequência de caracteres reconhecidos;
- 8.50.19. Deve permitir a busca de múltiplos veículos dentro de uma única busca, dentro de um critério único;
- 8.50.20. Deve ser capaz de pesquisar pela câmera que realizou o reconhecimento de placa;
- 8.50.21. Deve ser capaz de pesquisar por qualquer sequência de caracteres reconhecidos;
- 8.50.22. Deve permitir a configuração de alarmes e/ou eventos baseados no reconhecimento de placas;
- 8.50.23. Deve ter capacidade de integrar com o Sistema de Controle de Acesso obtido através deste edital para permitir o acionamento das cancelas após o reconhecimento da placa veicular;
- 8.50.24. Deve ser compatível com Microsoft® Windows® Server 2016 ou versão mais recente;

**8.51. SERVIÇO DE PLANEJAMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE GERENCIAMENTO DE VIDEOMONITORAMENTO VMS**

- 8.51.1. Serviço de instalação de software VMS compreende:
- 8.51.2. Instalação do software VMS no servidor designado para este fim;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.51.3. Serviço de configurações de software VMS compreendem:
- 8.51.4. Configurações básicas para que o software entre em operação no ambiente proposto, adição das câmeras IP, atribuição de nome, atribuição de IP, configurações de imagens, resolução, qualidade de imagem, streamings de vídeo, configurações de armazenamento, gravação e configurações gerais;
- 8.51.5. Devem ser instaladas e implantados os protocolos e serviços necessários e suficientes para ativação e operação das funcionalidades e a configuração do software VMS, explorando suas características, a seguir descritas, dentro das melhores práticas de rede, comunicação, segurança, disponibilidade, integridade e confiabilidade da informação;

**8.52. RACK DE PISO**

- 8.52.1. Fornecimento de rack com as seguintes especificações:
  - 8.52.1.1. Deve possuir altura de 44U, padrão 19” e profundidade mínima de 670mm;
  - 8.52.1.2. Deve possuir porta frontal em vidro de 5mm, temperado e serigrafado com fecho cilindro e chaves;
  - 8.52.1.3. Deve possuir estrutura monobloco em chapa de aço;
  - 8.52.1.4. Deve possuir planos de montagem com marcação em meio “U” e regulagem na profundidade em chapa de aço 1,5mm;
  - 8.52.1.5. Deve possuir teto removível em chapa de aço 0,75mm com aletas para ventilação e predisposição para instalação de 4 micro ventiladores;
  - 8.52.1.6. Deve possuir laterais e fundo removíveis e bipartida na horizontal em chapa de aço 0,75mm com fecho cilindro e chaves;
  - 8.52.1.7. Deve possuir base soleira em chapa de aço 1,5mm, para acomodação de reserva técnica de cabos;
  - 8.52.1.8. Deve possuir abertura destacável no teto e na base para passagem de cabos na parte traseira e pés niveladores;
  - 8.52.1.9. Deve possuir pintura eletrostática a pó na cor preta e ser fornecido com os seguintes acessórios:
    - 8.52.1.9.1. Parafuso porca gaiola para todas as unidades de U’s;
    - 8.52.1.9.2. Fornecido com 2 réguas com no mínimo 8 tomadas 10 ou 20A;

**8.53. SERVIÇO DE INSTALAÇÃO DE RACK DE PISO**

- 8.53.1. A instalação de rack compreende todos os procedimentos necessários para tornar o armário de telecomunicação em estado operacional, incluindo as seguintes atividades e materiais:
- 8.53.2. Serviço de fixação do armário, conforme orientações do fabricante.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.53.3. Serviço de perfuração das superfícies (paredes e divisórias).
- 8.53.4. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.53.5. Serviço de fixação e acomodação de todos os equipamentos e demais componentes dentro do rack.
- 8.53.6. Serviço de instalação da régua de tomadas elétricas no rack, em conformidade com as orientações do fabricante.
- 8.53.7. Serviço de organização do cabeamento dentro do rack, atendendo às normas técnicas vigentes, bem como recomendações do fabricante e orientações da contratante.
- 8.53.8. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície;
- 8.53.9. Apresentar catálogo do fabricante para comprovação de atendimento às especificações mínimas aqui exigidas; Serviço de fixação do armário, conforme orientações do fabricante.
- 8.53.10. Serviço de perfuração das superfícies (paredes e divisórias).
- 8.53.11. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.53.12. Serviço de fixação e acomodação de todos os equipamentos e demais componentes dentro do rack.
- 8.53.13. Serviço de instalação da régua de tomadas elétricas no rack, em conformidade com as orientações do fabricante.
- 8.53.14. Serviço de organização do cabeamento dentro do rack, atendendo às normas técnicas vigentes, bem como recomendações do fabricante e orientações da contratante.
- 8.53.15. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície;
- 8.53.16. Apresentar catálogo do fabricante para comprovação de atendimento às especificações mínimas aqui exigidas;

**8.54. RACK DE TETO**

- 8.54.1. Fornecimento de rack de teto com as seguintes especificações:
  - 8.54.1.1. Deve possuir altura de 5U's padrão 19";
  - 8.54.1.2. Deve possuir as seguintes dimensões aproximadas: 596mm x 596mmx

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
341mm;

- 8.54.1.3. Deve ser fabricado em Aço e possuir capacidade mínima de carga de 22kgç
- 8.54.1.4. Deve ser projetado para instalação no teto;
- 8.54.1.5. Deve possuir porta articulada com ventilador de exaustão 110V integrado;
- 8.54.1.6. Deve possuir pistões a gás para retenção de carga na porta em abertura;
- 8.54.1.7. Deve possuir abertura para entrada e saída de cabos;
- 8.54.1.8. Deve possuir em seu corpo quatro suportes para fixação de tirantes possibilitando assim seu nivelamento com o forro;
- 8.54.1.9. Deve possuir pintura na cor branca;
- 8.54.1.10. Deve ser projetado para acomodar equipamentos ativos e passivos de rede;

#### **8.55. SERVIÇO DE INSTALAÇÃO DE RACK DE TETO**

- 8.55.1. A instalação de rack de teto compreende todos os procedimentos necessários para tornar o armário de telecomunicação em estado operacional, incluindo as seguintes atividades:
- 8.55.2. Serviço de fixação do armário, conforme orientações do fabricante.
- 8.55.3. Serviço de perfuração das superfícies (paredes e divisórias).
- 8.55.4. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.55.5. Serviço de fixação e acomodação de todos os equipamentos e demais componentes dentro do rack.
- 8.55.6. Serviço de instalação da régua de tomadas elétricas no rack, em conformidade com as orientações do fabricante.
- 8.55.7. Serviço de organização do cabeamento dentro do rack, atendendo às normas técnicas vigentes, bem como recomendações do fabricante e orientações da contratante.
- 8.55.8. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície;
- 8.55.9. Apresentar catálogo do fabricante para comprovação de atendimento às especificações mínimas aqui exigidas;

#### **8.56. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ELETROCALHA**

- 8.56.1. A instalação do metro de eletrocalha compreende todos os procedimentos

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
necessários para disponibilizar a passagem adequada de cabos de rede entre o rack e os pontos de consolidação, incluindo as seguintes atividades e materiais:

- 8.56.2. Fornecimento de eletrocalha, com as seguintes especificações:
- 8.56.2.1. Deve possuir dimensões mínimas de 50mm x 50mm x 3m e máxima de 150mm x 50mm x 3m;
  - 8.56.2.2. Deve ser do modelo do tipo “U”, sem abas e perfurada;
  - 8.56.2.3. Deve possuir tratamento de toda sua superfície e acessórios associados por sistema pré-zincado a fogo, por imersão;
  - 8.56.2.4. Deve possuir sistema de junção rápida ou sistemas de fixação para parafusos;
  - 8.56.2.5. Fornecimento de tampa e septo divisor.
  - 8.56.2.6. Fornecimento de acessórios metálicos, conforme a necessidade (curvas, tês, cruzetas, desvios, junções, cotovelos, reduções, flanges, saídas, terminais e suportes);
  - 8.56.2.7. Todos os acessórios devem obedecer às mesmas características construtivas da barra de eletrocalha, porém, suas formas geométricas são próprias, atendendo às mais diversas situações de montagem e distribuição, conforme orientação do fabricante;
  - 8.56.2.8. Fornecimento de parafusos com buchas, conforme a superfície existente;
- 8.56.3. Fornecimento de materiais de acabamento, se aplicável, conforme a superfície perfurada ou transposta (massa, gesso, cimento, selador e tinta).
- 8.56.4. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície.
- 8.56.5. Apresentar catálogo do fabricante comprovando o atendimento às características técnicas aqui exigidas.;

## **8.57. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE SEAL TUBE TIPO I**

- 8.57.1. A instalação do metro de conduíte tipo sealtubo compreende todos os procedimentos necessários para disponibilizar a passagem adequada de cabos dos pontos de consolidação à estação de trabalho dos usuários, incluindo as seguintes atividades e materiais:
- 8.57.1.1. Fornecimento de conduíte tipo sealtubo auto extingüível com as seguintes especificações:
  - 8.57.1.2. Deverá possuir diâmetro ¾”
  - 8.57.1.3. Deverá ser fabricado em espiral, com fita de aço zincado e revestido

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
externamente com PVC extrudado;

- 8.57.1.4. Fornecimento de acessórios, conforme a necessidade (curvas, box curvo, box reto, buchas, arruelas, luvas);
- 8.57.1.5. Fornecimento de parafusos com buchas, conforme a superfície existente;
- 8.57.1.6. Serviço de fixação das mangueiras, conduítes ou tubos e respectivos acessórios.
- 8.57.1.7. Serviço de recorte das mangueiras, conduítes ou tubos.
- 8.57.1.8. Serviço de transposição de paredes, laje, forro ou divisória.
- 8.57.1.9. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície.
- 8.57.1.10. Apresentar catálogo do fabricante;

## **8.58. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE SEAL TUBE TIPO II**

- 8.58.1. A instalação do metro de conduíte tipo sealtubo compreende todos os procedimentos necessários para disponibilizar a passagem adequada de cabos dos pontos de consolidação à estação de trabalho dos usuários, incluindo as seguintes atividades e materiais:
  - 8.58.1.1. Fornecimento de conduíte tipo sealtubo auto extingüível com as seguintes especificações:
  - 8.58.1.2. Deverá possuir diâmetro de 1”;
  - 8.58.1.3. Deverá ser fabricado em espiral, com fita de aço zincado e revestido externamente com PVC extrudado;
  - 8.58.1.4. Fornecimento de acessórios, conforme a necessidade (curvas, box curvo, box reto, buchas, arruelas, luvas);
  - 8.58.1.5. Fornecimento de parafusos com buchas, conforme a superfície existente;
  - 8.58.1.6. Serviço de fixação das mangueiras, conduítes ou tubos e respectivos acessórios.
  - 8.58.1.7. Serviço de recorte das mangueiras, conduítes ou tubos.
  - 8.58.1.8. Serviço de transposição de paredes, laje, forro ou divisória.
  - 8.58.1.9. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
na superfície.

8.58.1.10. Apresentar catálogo do fabricante;

### **8.59. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CANALETA TIPO I**

8.59.1. A instalação do metro de canaleta compreende todos os procedimentos necessários para disponibilizar a passagem adequada de cabos dos pontos de consolidação à estação de trabalho dos usuários, incluindo as seguintes atividades e materiais, conforme a necessidade:

8.59.2. Fornecimento de canaleta fechada para aplicação em piso, com as seguintes especificações:

8.59.2.1. Devera possuir dimensões mínimas de 60x30mm (Largura x Altura);

8.59.2.2. Deverá ser de material Cloreto de Polivinila rígido resistente a risco, lascas e corrosão;

8.59.2.3. Deverá ser de cor branca quando não existir canaleta no local e na existência de infraestrutura do seguimento na mesma cor/padrão dos demais produtos do seguimento de infraestrutura;

8.59.2.4. Deverá ser obrigatoriamente não metálico, multicanal com o objetivo de distribuir, e proteger os cabos de dados, voz, vídeo, fibra ótica e cabos de circuitos alimentadores.

8.59.2.5. Deverá respeitar o raio de curvatura dos cabos a serem instalados, com no mínimo de 1", de acordo com TIA/EIA-568-B. Deve ser aprovado pela UL 94-0 de flamabilidade.

8.59.2.6. Deverá ser provido de tampa altamente resistente, no sentido de dificultar a abertura da canaleta e com isso impedir a ação indevida do uso das mesmas.

8.59.2.7. Deverá ser provido de separação interna ajustável, no sentido de maximizar o uso das áreas exclusivas para os diferentes tipos de cabos a serem colocados (vídeo, voz, dados e elétrica),

8.59.2.8. Deverá ser provido de todas os acessórios para completar o sistema de canaletas, com o objetivo de providenciar a instalação sem o uso de "gambiarras", terminações, emendas, retentores de fios, materiais de fixação e demais acessórios, que deverão ser embutidos nos custos necessários.

8.59.2.9. Deverá ser apropriado para o uso nas aplicações até 600 volts entre condutores;

8.59.3. Apresentar catálogo do fabricante;

8.59.4. Deve ser fornecida com todos os acessórios necessários para fixação em parede como parafuso, bucha, arruela e fixa cabos.

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

- 8.59.5. Fornecimento de materiais de acabamento, se aplicável, conforme a superfície perfurada (massa, gesso, cimento, selador e tinta).
- 8.59.6. Serviço de fixação das canaletas e respectivos acessórios.
- 8.59.7. Serviço de recorte das canaletas.
- 8.59.8. Serviço de perfuração das superfícies (paredes, divisórias e/ou mesas).
- 8.59.9. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.59.10. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície.

**8.60. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CANALETA TIPO II**

- 8.60.1. A instalação do metro de canaleta compreende todos os procedimentos necessários para disponibilizar a passagem adequada de cabos dos pontos de consolidação à estação de trabalho dos usuários, incluindo as seguintes atividades e materiais, conforme a necessidade:
- 8.60.2. Fornecimento de canaleta fechada para aplicação em piso, com as seguintes especificações:
  - 8.60.2.1. Devera possuir dimensões mínimas de 100x44mm (Largura x Altura);
  - 8.60.2.2. Deverá ser de material Cloreto de Polivinila rígido resistente a risco, lascas e corrosão;
  - 8.60.2.3. Deverá ser de cor branca quando não existir canaleta no local e na existência de infraestrutura do seguimento na mesma cor/padrão dos demais produtos do seguimento de infraestrutura;
  - 8.60.2.4. Deverá ser obrigatoriamente não metálico, multicanal com o objetivo de distribuir, e proteger os cabos de dados, voz, vídeo, fibra ótica e cabos de circuitos alimentadores.
  - 8.60.2.5. Deverá respeitar o raio de curvatura dos cabos a serem instalados, com no mínimo de 1", de acordo com TIA/EIA-568-B. Deve ser aprovado pela UL 94-0 de flamabilidade.
  - 8.60.2.6. Deverá ser provido de tampa altamente resistente, no sentido de dificultar a abertura da canaleta e com isso impedir a ação indevida do uso das mesmas.
  - 8.60.2.7. Deverá ser provido de separação interna ajustável, no sentido de maximizar o uso das áreas exclusivas para os diferentes tipos de cabos a serem colocados (vídeo, voz, dados e elétrica),

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

- 8.60.2.8. Deverá ser provido de todas os acessórios para completar o sistema de canaletas, com o objetivo de providenciar a instalação sem o uso de “gambiarras”, terminações, emendas, retentores de fios, materiais de fixação e demais acessórios, que deverão ser embutidos nos custos necessários.
- 8.60.2.9. Deverá ser apropriado para o uso nas aplicações até 600 volts entre condutores;
- 8.60.3. Apresentar catálogo do fabricante;
- 8.60.4. Deve ser fornecida com todos os acessórios necessários para fixação em parede como parafuso, bucha, arruela e fixa cabos.
- 8.60.5. Fornecimento de materiais de acabamento, se aplicável, conforme a superfície perfurada (massa, gesso, cimento, selador e tinta).
- 8.60.6. Serviço de fixação das canaletas e respectivos acessórios.
- 8.60.7. Serviço de recorte das canaletas.
- 8.60.8. Serviço de perfuração das superfícies (paredes, divisórias e/ou mesas).
- 8.60.9. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.60.10. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície.

**8.61. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA EXTERNA COM ESPELHO TIPO I**

- 8.61.1. A instalação da unidade de caixa de superfície, com espelho para conectores RJ45, compreende todos os procedimentos necessários para disponibilizar pontos de rede lógica para estações de trabalho dos usuários, incluindo as seguintes atividades e materiais, conforme a necessidade:
- 8.61.2. Fornecimento de caixa de superfície, com as seguintes especificações:
- 8.61.2.1. A caixa de superfície deverá ser obrigatoriamente não metálica, multicanal com o objetivo de distribuir, e proteger os cabos de dados, voz, vídeo, fibra ótica e cabos de circuitos alimentadores;
- 8.61.2.2. Deverá ser apropriado para o uso nas aplicações até 600 volts entre condutores;
- 8.61.2.3. Deverá ser fornecida caixa compatível com a canaleta ofertada com espelho para até 02 conectores RJ45;
- 8.61.2.4. Deve ser fabricada em material plástico UL94-V0, na cor branca;
- 8.61.2.5. Deve permitir encaixe rápido com garras de fixação e parafuso e bucha;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.61.3. Deve ser fornecida com todos os acessórios necessários para fixação em parede como parafuso, bucha, arruela e fixa cabos;
- 8.61.4. Fornecimento de tampas cegas para as posições do espelho que não forem utilizadas;
- 8.61.5. Serviço de perfuração das superfícies (paredes, divisórias e/ou mesas).
- 8.61.6. Serviço de acomodação dos cabos dentro da caixa de superfície, conforme orientação do fabricante.
- 8.61.7. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.61.8. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície.
- 8.61.9. Apresentar catálogo do fabricante;

**8.62. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA EXTERNA COM ESPELHO TIPO II**

- 8.62.1. A instalação da unidade de caixa de superfície, com espelho para conectores ópticos SC, compreende todos os procedimentos necessários para disponibilizar pontos de fibra óptica para estações de trabalho dos usuários, incluindo as seguintes atividades e materiais, conforme a necessidade:
- 8.62.2. Fornecimento de caixa de superfície, com as seguintes especificações:
  - 8.62.2.1. A caixa de superfície deverá ser obrigatoriamente não metálica, multicanal com o objetivo de distribuir, e proteger os cabos de dados, voz, vídeo, fibra ótica e cabos de circuitos alimentadores;
  - 8.62.2.2. Deverá ser apropriado para o uso nas aplicações até 600 volts entre condutores;
  - 8.62.2.3. Deverá ser fornecida caixa compatível com a canaleta ofertada com espelho para até 03 tomadas 2P+T;
  - 8.62.2.4. Deve ser fabricada em material plástico UL94-V0, na cor branca;
  - 8.62.2.5. Deve permitir encaixe rápido com garras de fixação e parafuso e bucha;
- 8.62.3. Deve ser fornecida com todos os acessórios necessários para fixação em parede como parafuso, bucha, arruela e fixa cabos;
- 8.62.4. Fornecimento de tampas cegas para as posições do espelho que não forem utilizadas;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.62.5. Serviço de perfuração das superfícies (paredes, divisórias e/ou mesas).
- 8.62.6. Serviço de acomodação dos cabos dentro da caixa de superfície, conforme orientação do fabricante.
- 8.62.7. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.62.8. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície.
- 8.62.9. Apresentar catálogo do fabricante;

**8.63. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ELETRODUTO METÁLICO**

- 8.63.1. A instalação da unidade da caixa de passagem compreende todos os procedimentos necessários para disponibilizar a passagem adequada de cabos, incluindo as seguintes atividades e materiais:
- 8.63.2. Fornecimento de eletroduto metálico rígido com as seguintes especificações:
  - 8.63.2.1. Deverá possuir tratamento anticorrosivo pelo sistema de banho químico (desengraxe e fosforização a base de fosfato de ferro) garantindo a resistência do produto;
  - 8.63.2.2. Deverá possuir dimensões mínimas de 200 x 200 x 100mm;
  - 8.63.2.3. Deverá possuir pintura à pó na cor bege ou Galvanizada.
- 8.63.3. Apresentar catálogo do fabricante;

**8.64. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA DE PASSAGEM METÁLICA**

- 8.64.1. A instalação do metro de eletroduto compreende todos os procedimentos necessários para disponibilizar a passagem adequada de cabos, incluindo as seguintes atividades e materiais:
  - 8.64.1.1. Fornecimento de eletroduto metálico rígido com as seguintes especificações:
  - 8.64.1.2. Fornecimento de eletroduto metálico rígido com diâmetro de 1”;
  - 8.64.1.3. Fornecimento de acessórios, conforme a necessidade (condutele, curvas, box curvo, box reto, buchas, arruelas, luvas);
  - 8.64.1.4. Fornecimento de parafusos com buchas, conforme a superfície existente;
  - 8.64.1.5. Serviço de fixação dos eletrodutos e respectivos acessórios.
  - 8.64.1.6. Serviço de recorte dos eletrodutos.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.64.1.7. Serviço de transposição de paredes, laje, forro ou divisória.
- 8.64.1.8. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície.
- 8.64.1.9. Apresentar catálogo do fabricante;

**8.65. RACK DE PAREDE 12U**

- 8.65.1. Fornecimento de rack de parede 12U com as seguintes especificações:
  - 8.65.1.1. Deverá possuir porta frontal em vidro temperado de 4mm, serigrafado com fecho cilindro e chave;
  - 8.65.1.2. Deverá possuir estrutura monobloco em chapa de aço;
  - 8.65.1.3. Deverá possuir profundidade mínima de 550mm ser padrão 19”x12U;
  - 8.65.1.4. Deverá possuir planos de montagem com marcação em meio “U” e regulagem em profundidade;
  - 8.65.1.5. Deverá possuir teto com predisposição para dois ventiladores;
  - 8.65.1.6. Deverá possuir laterais removíveis e com aletas para ventilação e fecho rápido;
  - 8.65.1.7. Deverá possuir abertura para entrada e saída de cabos no teto e base.
  - 8.65.1.8. Deverá possuir pintura eletrostática a pó na cor preta.
  - 8.65.1.9. Deverá ser fornecido com os seguintes acessórios:
    - 8.65.1.9.1. 48 parafusos porca gaiola;
    - 8.65.1.9.2. 04 painéis de fechamento cego 19”x1U;
    - 8.65.1.9.3. 04 organizadores de cabo 19”x1U;
    - 8.65.1.9.4. Parafusos e buchas para fixação de rack em parede, teto ou divisória.
    - 8.65.1.9.5. Régua de 06 tomadas 2P+T.

**8.66. SERVIÇO DE INSTALAÇÃO DE RACK DE PAREDE 12U**

- 8.66.1. A instalação de rack de parede 12U compreende os procedimentos necessários para tornar o armário de telecomunicação em estado operacional, incluindo as seguintes atividades:
- 8.66.2. Serviço de fixação do armário, conforme orientações do fabricante.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.66.3. Serviço de perfuração das superfícies (paredes e divisórias).
- 8.66.4. Serviço de transposição de parede, laje, forro ou divisória, conforme a necessidade.
- 8.66.5. Serviço de fixação e acomodação de os equipamentos e demais componentes dentro do rack.
- 8.66.6. Serviço de instalação da régua de tomadas elétricas no rack, em conformidade com as orientações do fabricante.
- 8.66.7. Serviço de organização do cabeamento dentro do rack, atendendo às normas técnicas vigentes, bem como recomendações do fabricante e orientações da contratante.
- 8.66.8. Serviço de acabamento da superfície perfurada e/ou transposta, conforme necessidade: preparação; preenchimento com massa/gesso/cimento; lixamento; aplicação de selador; e pintura, utilizando a mesma cor existente na superfície;
- 8.66.9. Apresentar catálogo do fabricante.

**8.67. SERVIÇO DE INSTALAÇÃO DE PONTO COM FORNECIMENTO DE CABEAMENTO ESTRUTURADO CATEGORIA 6A**

- 8.67.1. A instalação do ponto de cabeamento estruturado categoria 6A compreende os procedimentos necessários para lançamento de cabeamento do ponto de consolidação à estação de trabalho do usuário ou ao rack de telecomunicação, incluindo as seguintes atividades e materiais:
- 8.67.2. Deve contemplar o lançamento de cabos, conector cat. 6A, e crimpagem em ambas as pontas bem como, identificação e testes.
- 8.67.3. Fornecimento de cabo UTP cat. 6A com as seguintes especificações:
- 8.67.4. Deve possuir 4 pares de cabos trançados de cobre nu;
- 8.67.5. Deve possuir a medida de área 23AWG e ser fornecido em bobinas de 305m;
- 8.67.6. Deve ser recoberto por fita metálica com recortes a laser que garanta imunidade a alien crossalk, garantindo performance em transmissões 10Gbps.
- 8.67.7. Classe de flamabilidade LSZH;
- 8.67.8. Deve possuir capa externa em PVC não propagante à chama conforme normas vigentes;
- 8.67.9. Compatível com aplicações POE:
- 8.67.10. IEEE 802.3af

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

8.67.11. IEEE 802.3at

8.67.12. IEEE 8023.bt

8.67.13. Deve estar em conformidade com as diretivas RoHs para metais pesados;

8.67.14. Deve estar em conformidade com as seguintes normas:

8.67.15. ANSI/TIA-568-C.2 Category 6A;

8.67.16. ISO 11801 Class EA;

8.67.17. IEC 61156-5 Category 6A;

8.67.18. Certificação ETL para teste de canal com 4 conexões.

8.67.19. Deve possuir marcação sequencial métrica;

8.67.20. Fornecimento de conector RJ45 fêmea CAT 6 A com as seguintes especificações:

8.67.21. Deve possuir 8 vias em bronze fosforoso com 50 $\mu$ m (1,27 $\mu$ m) de ouro e 100 $\mu$ m (2,54 $\mu$ m) de níquel;

8.67.22. Deve ser em fabricado com corpo termoplástico não propagante a chama UL 94V-0;

8.67.23. Deve possuir sistema de rastreamento do produto através de embalagem com código do produto, data de fabricação e contato do fabricante;

8.67.24. Deve utilizar sistema de terminação sem uso de ferramenta de impacto (punch-down).

8.67.25. Deve permitir até 20 reterminações possibilitando mudanças de layout com reaproveitamento do mesmo conector.

8.67.26. Compatível com aplicações POE:

8.67.27. IEEE 802.3af

8.67.28. IEEE 802.3at

8.67.29. IEEE 8023.bt, tipo 3 e tipo 4.

8.67.30. Deve ser compatível com cabos sólidos de 22 a 26AWG;

8.67.31. Deve estarem conformidade com as diretivas RoHs para metais pesados;

8.67.32. Deve estar em conformidade com a norma EIA/TIA 568 C.2 Category 6A;

8.67.33. Deve estar em conformidade com UL 1863 e UL2043;

8.67.34. Serviço de lançamento do cabo, percorrendo toda a infraestrutura, em

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
conformidade atendendo às normas técnicas e recomendações do fabricante;

- 8.67.35. Serviço de crimpagem do conector ao cabo, conforme as orientações do fabricante;
- 8.67.36. Caso o fabricante disponha de ferramenta específica para instalação do conector, a mesma deverá ser utilizada;
- 8.67.37. Os cabos e conectores a serem fornecidos, para composição do ponto de cabeamento categoria 6A, devem ser de um mesmo fabricante para garantir a interoperabilidade dos produtos entre si e possibilidade de garantia estendida.
- 8.67.38. Todo o cabeamento estruturado categoria 6A deverá ser certificado para possuir garantia do fabricante de 25 anos do link permanente.

#### **8.68. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH PANEL MODULAR CATEGORIA 6ª**

- 8.68.1. A instalação da unidade de patch panel compreende os procedimentos necessários para a disponibilização do mesmo no rack, incluindo as seguintes atividades e materiais:
- 8.68.2. Fornecimento de patch panel descarregado modular com as seguintes especificações:
- 8.68.3. Patch Panel Descarregado;
- 8.68.4. Deve ser modular reto ou angular, multimídia, com 24 portas;
- 8.68.5. Compatível com conectores RJ45 de categoria 6 e 6A e conectores tipo A/V;
- 8.68.6. Deve apresentar corpo metálico e serem fornecidos com 6 módulos em ABS, cada módulo deve suportar até 4 conectores;
- 8.68.7. Os módulos devem possibilitar remoção pela parte frontal do patch panel;
- 8.68.8. Deve possibilitar a substituição de conectores individualmente;
- 8.68.9. Montagem em racks padrão EIA 19”;
- 8.68.10. Deve ser fornecido com etiqueta para identificação das portas compatível com TIA/EIA 606-A;
- 8.68.11. Acabamento em pintura epóxi de alta resistência a riscos na cor preta resistente e protegido contra corrosão;
- 8.68.12. Deve ser do mesmo fabricante do item 13 a fim de garantir a interoperabilidade dos produtos entre si;
- 8.68.13. A posição no rack deve ser definida de forma a minimizar o comprimento dos patchs cords;
- 8.68.14. Serviço de instalação do patch panel no rack, em conformidade com as orientações

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
do fabricante.

**8.69. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD  
RJ45 CATEGORIA 6A - TIPO I**

- 8.69.1. A instalação com fornecimento de patch cord compreende os procedimentos necessários para disponibilizar o link de dados, incluindo as seguintes atividades e materiais:
- 8.69.2. Fornecimento de patch cord com as seguintes especificações:
- 8.69.3. Devera possuir comprimento mínimo de 1,5m;
- 8.69.4. Devem exceder e superar as recomendações da TIA/EIA-568.2-D para categoria 6A;
- 8.69.5. Devem ser testados e aprovados pelo ETL para categoria 6A.
- 8.69.6. Deve ser recoberto por fita metálica com recortes a laser que garanta imunidade a alien crossalk, garantindo performance em transmissões 10Gbps;
- 8.69.7. Devem ser construídos com conectores macho (plugs) tipo RJ45 em ambas as extremidades. O cabo utilizado para estes patches cords deverá ser cabo sólido categoria 6A, de no mínimo 24 AWG de cobre em par trançado;
- 8.69.8. Compatível com aplicações POE considerando os padrões abaixo:
- 8.69.9. IEEE 802.3af;
- 8.69.10. IEEE 802.3at;
- 8.69.11. IEEE 8023.bt, tipo 3 e tipo 4;
- 8.69.12. O conector deve ser desenhado com um mecanismo integral de bloqueio que proteja o ajuste mecânico da conexão (lingüetas) contra fígamento acidental, ao qual depois de haver sido inserido, sirva de proteção para não ser extraído de forma acidental;
- 8.69.13. Os plugs devem contar com tecnologia de-embeded de acordo a TIA/EIA 568.2-D;
- 8.69.14. Os patches cords deverão ter um sistema que controle a tensão a que se submetem no processo de instalação. Este sistema deve ser parte integral do processo de fabricação do patch cord na planta do fabricante. Este sistema deve preservar o raio de curvatura de 1” ao ser inserido o plug no conector;
- 8.69.15. Todos os patches cords deverão ser originais de fábrica, elaborados e construídos pelo mesmo fabricante da conectividade e pré-certificados como estipulado na TIA/EIA, e deverão vir em suas bolsas originais de empacotamento tal como saem da fábrica.
- 8.69.16. Deve ser original de fábrica e previamente certificados, em conformidade com a

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
normativa TIA/EIA-568-C.2-1 para categoria 6A;

- 8.69.17. Deve ser do mesmo fabricante do item 13 a fim de garantir a interoperabilidade dos produtos entre si;
- 8.69.18. Serviço de instalação do patch cord no rack, no ponto de consolidação ou na área de trabalho, atendendo às recomendações do fabricante, bem como normas técnicas vigentes

#### **8.70. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO II**

- 8.70.1. A instalação com fornecimento de patch cord compreende os procedimentos necessários para disponibilizar o link de dados, incluindo as seguintes atividades e materiais:
- 8.70.2. Fornecimento de patch cord com as seguintes especificações:
- 8.70.3. Devera possuir comprimento mínimo de 3m;
- 8.70.4. Devem exceder e superar as recomendações da TIA/EIA-568.2-D para categoria 6A.
- 8.70.5. Devem ser testados e aprovados pelo ETL para categoria 6A.
- 8.70.6. Deve ser recoberto por fita metálica com recortes a laser que garanta imunidade a alien crossalk, garantindo performance em transmissões 10Gbps.
- 8.70.7. Devem ser construídos com conectores macho (plugs) tipo RJ45 em ambas as extremidades. O cabo utilizado para estes patch cords deverá ser cabo sólido categoria 6A, de no mínimo 24 AWG de cobre em par trançado.
- 8.70.8. Compatível com aplicações POE, considerando os padrões abaixo:
- 8.70.9. IEEE 802.3af
- 8.70.10. IEEE 802.3at
- 8.70.11. IEEE 8023.bt, tipo 3 e tipo 4.
- 8.70.12. O conector deve ser desenhado com um mecanismo integral de bloqueio que proteja o ajuste mecânico da conexão (lingüetas) contra fígamento acidental, ao qual depois de haver sido inserido, sirva de proteção para não ser extraído de forma acidental.
- 8.70.13. Os plugs devem contar com tecnologia de-embeded de acordo a TIA/EIA 568.2-D.
- 8.70.14. Os patch cords deverão ter um sistema que controle a tensão a que se submetem no processo de instalação. Este sistema deve ser parte integral do processo de fabricação do patch cord na planta do fabricante. Este sistema deve preservar o

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
raio de curvatura de 1” ao ser inserido o plug no conector.

- 8.70.15. Todos os patch cords deverão ser originais de fábrica, elaborados e construídos pelo mesmo fabricante da conectividade e pré-certificados como estipulado na TIA/EIA, e deverão vir em suas bolsas originais de empacotamento tal como saem da fábrica.
- 8.70.16. Deve ser original de fábrica e previamente certificados, em conformidade com a normativa TIA/EIA-568-C.2-1 para categoria 6;
- 8.70.17. Deve ser do mesmo fabricante do item 13 a fim de garantir a interoperabilidade dos produtos entre si;
- 8.70.18. Serviço de instalação do patch cord no rack, no ponto de consolidação ou na área de trabalho, atendendo às recomendações do fabricante, bem como normas técnicas vigentes.

#### **8.71. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD RJ45 CATEGORIA 6A - TIPO III**

- 8.71.1. A instalação com fornecimento de patch cord compreende os procedimentos necessários para disponibilizar o link de dados, incluindo as seguintes atividades e materiais:
- 8.71.2. Fornecimento de patch cord com as seguintes especificações:
- 8.71.3. Devera possuir comprimento mínimo de 5m;
- 8.71.4. Devem exceder e superar as recomendações da TIA/EIA-568.2-D para categoria 6A.
- 8.71.5. Devem ser testados e aprovados pelo ETL para categoria 6A.
- 8.71.6. Deve ser recoberto por fita metálica com recortes a laser que garanta imunidade a alien crossalk, garantindo performance em transmissões 10Gbps.
- 8.71.7. Devem ser construídos com conectores macho (plugs) tipo RJ45 em ambas as extremidades. O cabo utilizado para estes patch cords deverá ser cabo sólido categoria 6A, de no mínimo 24 AWG de cobre em par trançado.
- 8.71.8. Compatível com aplicações POE, considerando os padrões abaixo:
- 8.71.9. IEEE 802.3af
- 8.71.10. IEEE 802.3at
- 8.71.11. IEEE 8023.bt, tipo 3 e tipo 4.
- 8.71.12. O conector deve ser desenhado com um mecanismo integral de bloqueio que proteja o ajuste mecânico da conexão (lingüetas) contra físgamento acidental, ao qual depois de haver sido inserido, sirva de proteção para não ser extraído de forma acidental.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.71.13. Os plugs devem contar com tecnologia de-embeded de acordo a TIA/EIA 568.2-D.
- 8.71.14. Os patch cords deverão ter um sistema que controle a tensão a que se submetem no processo de instalação. Este sistema deve ser parte integral do processo de fabricação do patch cord na planta do fabricante. Este sistema deve preservar o raio de curvatura de 1” ao ser inserido o plug no conector.
- 8.71.15. Todos os patch cords deverão ser originais de fábrica, elaborados e construídos pelo mesmo fabricante da conectividade e pré-certificados como estipulado na TIA/EIA, e deverão vir em suas bolsas originais de empacotamento tal como saem da fábrica.
- 8.71.16. Deve ser original de fábrica e previamente certificados, em conformidade com a normativa TIA/EIA-568-C.2-1 para categoria 6;
- 8.71.17. Deve ser do mesmo fabricante do item 13 a fim de garantir a interoperabilidade dos produtos entre si;
- 8.71.18. Serviço de instalação do patch cord no rack, no ponto de consolidação ou na área de trabalho, atendendo às recomendações do fabricante, bem como normas técnicas vigentes.

**8.72. SERVIÇO DE CERTIFICAÇÃO DE PONTO LÓGICO**

- 8.72.1. Deverá fazer a certificação de Ponto Lógico com Scanner (Bidirecional) próprio para categoria, Impressão do Relatório de Certificação, Encadernação do Relatório de Certificação, Conferência e assinatura dos Relatórios;
- 8.72.2. A Certificação do ponto deverá atender aos seguintes itens;
- 8.72.3. Os testes em cabos de par trançado blindado e não blindado (UTP e STP) deverão ser realizados com aparelho de certificação recomendados, por norma, para as categorias Cat. 6 e Cat. 6a.;
- 8.72.4. Deverão ser fornecidos os certificados de calibração dos aparelhos de certificação utilizados com, no mínimo, um ano de validade;
- 8.72.5. As instalações deverão ser certificadas com base na norma NBR-14565 e EIA/TIA-568 B, verificando-se, para as categorias 5e, 6 e 6a;
- 8.72.6. Correta conexão de todos os pinos-mapa de fios (Wire map.);
- 8.72.7. Comprimento máximo dos cabos dentro da norma-100m [90m de cabo fixo + 10m patch cords] (Length); Resistência (Resistance);
- 8.72.8. Atenuação (Attenuation);
- 8.72.9. Atraso de Propagação (Propagation Delay);
- 8.72.10. Desvio do Retardo (Delay Skew);

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.72.11. Perda de Retorno (Return Loss);
- 8.72.12. Perda de Inserção (Insertion Loss);
- 8.72.13. NEXT (Near End Crosstalk);
- 8.72.14. PS NEXT (Power Sum Near End Crosstalk);
- 8.72.15. ACR ou ACRN (Attenuation to Crosstalk Ratio – Extremidade Próxima);
- 8.72.16. PS ACR ou PS ACR-N (Power Sum Attenuation to Crosstalk Ratio – Extremidade Próxima);
- 8.72.17. FEXT (Far End Crosstalk);
- 8.72.18. ELFEXT (Equal Level Far End Crosstalk) ou ACRF (Attenuation to Crosstalk Ratio – Extremidade Distante);
- 8.72.19. Distantemente);
- 8.72.20. PS ELFEXT (Power Sum Equal Level Far End Crosstalk) ou PS ACRF (Power Sum Attenuation to Crosstalk Ratio – Extremidade Distante);
- 8.72.21. Adicionam-se para a categoria 6a, os seguintes parâmetros;
- 8.72.22. Alien Crosstalk (AXTalk);
- 8.72.23. Power Sum Alien NEXT (PS ANEXT);
- 8.72.24. Power Sum Alien Crosstalk Ratio – Extremidade Distante (PS AACRF);
- 8.72.25. Deverá apresentar os relatórios gerados pelo SCANNER, impressos em papel sulfite 75g formato A-4 assinados pelo Responsável Técnico da obra e em Pen Drive ou CD (compact Disk) em formato Adobe Acrobat (pdf);

**8.73. SERVIÇO DE REORGANIZAÇÃO DE RACKS ATÉ 25 PONTOS.**

- 8.73.1. Consiste em efetuar a reorganização no conjunto físico da rede que compreende os patchs cords, patch panel, voice panel, placas cegas, guias cabos e identificação de pontos lógicos no rack;
- 8.73.2. Deverão ser observados as melhores práticas de encaminhamento tais como evitar contato com cabos elétricos, curvaturas etc.

**8.74. SERVIÇO DE REORGANIZAÇÃO DE RACKS DE 25 ATÉ 50 PONTOS.**

- 8.74.1. Consiste em efetuar a reorganização no conjunto físico da rede que compreende os patch cords, patch panel, voice panel, placas cegas, guias cabos e identificação de pontos lógicos no rack;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.74.2. Deverão ser observados as melhores práticas de encaminhamento tais como evitar contato com cabos elétricos, curvaturas etc...

**8.75. SERVIÇO DE REORGANIZAÇÃO DE RACKS DE 50 ATÉ 100 PONTOS.**

- 8.75.1. Consiste em efetuar a reorganização no conjunto físico da rede que compreende os patchs cords, patch panel, voice panel, placas cegas, guias cabos e identificação de pontos lógicos no rack;
- 8.75.2. Deverão ser observados as melhores práticas de encaminhamento tais como evitar contato com cabos elétricos, curvaturas etc...

**8.76. SERVIÇO DE IDENTIFICAÇÃO DE PONTO LÓGICO**

- 8.76.1. Os cabeamentos horizontais deverão ser identificados, ou seja, deverá ser identificado a extremidade de cada cabo que deverá interligar os patch panels aos PCs, bem como, as extremidades dos cabos que interligarão as tomadas RJ-45 fêmeas aos Pcs;
- 8.76.2. Para identificação de todos os segmentos do cabeamento horizontal, deverá ser identificado os cabos UTP dentro da canaleta, patch panels e espelho do ponto ao qual o usuário conecta o patch cord. Deverá ser utilizada etiquetas com área de laminação para proteção da área impressa. Impressão gerada por impressora portátil de termo transferência com opção de comunicação com computador por porta USB, importação de dados de banco de dados ou planilha. Cartucho de etiquetas com autorreconhecimento da impressora, informando saldo de etiquetas restantes no cartucho. Todos os pontos lógicos, deverão ser identificados na parte frontal dos patchs panels, bem como, na porta etiqueta da caixa sobrepôr responsável pela fixação das tomadas RJ-45 fêmeas, utilizando o mesmo princípio da identificação do cabeamento horizontal.

**8.77. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE "DIO" PARA 12 FIBRAS MM OU SM**

- 8.77.1. A instalação da unidade de DIO para 12 fibras MM ou SM compreende os procedimentos necessários para a disponibilização do mesmo no rack, incluindo as seguintes atividades e materiais:
- 8.77.2. Fornecimento de DIO modular com as seguintes especificações:
- 8.77.3. Deve ser fornecido com Pig Tail, acopladores e demais acessórios necessários à instalação, fixação e identificação.
- 8.77.4. As Bandejas de fibra devem ser no mínimo uma unidade padrão de altura no rack (1U), ter a capacidade de abrigar até 36 vias de fibra;
- 8.77.5. As bandejas devem ser metálicas e completamente fechadas, contando com base, paredes laterais e tampa metálicas;
- 8.77.6. A tampa deve ser removível a fim de poder realizar manutenções, ampliações ou mudanças;
- 8.77.7. As bandejas deverão incluir os elementos de carretel para a reserva de fibra óptica;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.77.8. As bandejas devem contar com recortes para a inserção dos cabos de fibra óptica em pelo menos 03 de seus lados a fim de melhorar o manejo dos feixos de cabos;
- 8.77.9. Deverá ser colocada uma proteção plástica que impeça o contato do metal do corpo da bandeja com o cabo que ingressa na mesma;
- 8.77.10. Deverão ser fornecidos os elementos adequados para a fixação do cabo na bandeja;
- 8.77.11. A Bandeja deve permitir a instalação em seu interior de sub-bandejas para emendas mecânicas ou de fusão, a fim de garantir proteção do investimento;
- 8.77.12. Deve permitir a instalação de até 3 painéis modulares administráveis sobre os quais serão instalados os acopladores de Fibra padrão LC;
- 8.77.13. Não serão aceitos painéis para acopladores que não permitam a instalação no futuro de outro tipo de acopladores;
- 8.77.14. Devem ser colocadas tampas cegas em todas as posições não utilizadas do painel de Fibra Óptica;
- 8.77.15. Serviço de fixação do DIO no rack, em conformidade com as recomendações do fabricante.
- 8.77.16. Apresentar catálogo do fabricante;

**8.78. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE "DIO" PARA 72 FIBRAS MM OU SM**

- 8.78.1. A instalação da unidade de DIO para até 72 fibras MM ou SM compreende os procedimentos necessários para a disponibilização do mesmo no rack, incluindo as seguintes atividades e materiais:
- 8.78.2. Fornecimento de DIO modular com as seguintes especificações:
- 8.78.3. Deve ser fornecido com Pig Tail, acopladores e demais acessórios necessários à instalação, fixação e identificação.
- 8.78.4. As Bandejas de fibra devem ser no mínimo uma unidade padrão de altura no rack (1U), ter a capacidade de abrigar até 72 vias de fibra;
- 8.78.5. As bandejas devem ser metálicas e completamente fechadas, contando com base, paredes laterais e tampa metálicas;
- 8.78.6. A tampa deve ser removível a fim de poder realizar manutenções, ampliações ou mudanças;
- 8.78.7. As bandejas deverão incluir os elementos de carretel para a reserva de fibra óptica;
- 8.78.8. As bandejas devem contar com recortes para a inserção dos cabos de fibra óptica em pelo menos 03 de seus lados a fim de melhorar o manejo dos feixos de cabos;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.78.9. Deverá ser colocada uma proteção plástica que impeça o contato do metal do corpo da bandeja com o cabo que ingressa na mesma;
- 8.78.10. Deverão ser fornecidos os elementos adequados para a fixação do cabo na bandeja;
- 8.78.11. A Bandeja deve permitir a instalação em seu interior de sub-bandejas para emendas mecânicas ou de fusão, a fim de garantir proteção do investimento;
- 8.78.12. Deve permitir a instalação de até 6 painéis modulares administráveis sobre os quais serão instalados os acopladores de Fibra padrão LC;
- 8.78.13. Não serão aceitos painéis para acopladores que não permitam a instalação no futuro de outro tipo de acopladores;
- 8.78.14. Devem ser colocadas tampas cegas em todas as posições não utilizadas do painel de Fibra Óptica;
- 8.78.15. Serviço de fixação do DIO no rack, em conformidade com as recomendações do fabricante.
- 8.78.16. Apresentar catálogo do fabricante;
- 8.79. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CAIXA DE TERMINACAO OPTICA**
- 8.79.1. A instalação da unidade de DIO para até 72 fibras MM ou SM compreende os procedimentos necessários para a disponibilização do mesmo no rack, incluindo as seguintes atividades e materiais:
- 8.79.2. Fornecimento de DIO modular com as seguintes especificações:
- 8.79.3. Deve ser fornecido com Pig Tail, acopladores e demais acessórios necessários à instalação, fixação e identificação.
- 8.79.4. As Bandejas de fibra devem ser no mínimo uma unidade padrão de altura no rack (1U), ter a capacidade de abrigar até 72 vias de fibra;
- 8.79.5. As bandejas devem ser metálicas e completamente fechadas, contando com base, paredes laterais e tampa metálicas;
- 8.79.6. A tampa deve ser removível a fim de poder realizar manutenções, ampliações ou mudanças;
- 8.79.7. As bandejas deverão incluir os elementos de carretel para a reserva de fibra óptica;
- 8.79.8. As bandejas devem contar com recortes para a inserção dos cabos de fibra óptica em pelo menos 03 de seus lados a fim de melhorar o manejo dos feixos de cabos;
- 8.79.9. Deverá ser colocada uma proteção plástica que impeça o contato do metal do corpo da bandeja com o cabo que ingressa na mesma;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.79.10. Deverão ser fornecidos os elementos adequados para a fixação do cabo na bandeja;
- 8.79.11. A Bandeja deve permitir a instalação em seu interior de sub-bandejas para emendas mecânicas ou de fusão, a fim de garantir proteção do investimento;
- 8.79.12. Deve permitir a instalação de até 6 painéis modulares administráveis sobre os quais serão instalados os acopladores de Fibra padrão LC;
- 8.79.13. Não serão aceitos painéis para acopladores que não permitam a instalação no futuro de outro tipo de acopladores;
- 8.79.14. Devem ser colocadas tampas cegas em todas as posições não utilizadas do painel de Fibra Óptica;
- 8.79.15. Serviço de fixação do DIO no rack, em conformidade com as recomendações do fabricante.
- 8.79.16. Apresentar catálogo do fabricante;
- 8.80. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CABO DE FIBRA ÓPTICA INDOOR/OUTDOOR 06FO MM 50/125 OM3**
- 8.80.1. A instalação de cabeamento óptico óptica 06FO mm 50/125 OM3 uso interno ou externo compreende os procedimentos necessários para instalação do metro de cabo de fibra óptica, incluindo as seguintes atividades e materiais:
- 8.80.2. Fornecimento de cabo óptico 06FO mm 50/125 OM3 com as seguintes especificações:
- 8.80.3. Deve ser composto de 06 fibras ópticas e ser projetado para uso indoor/outdoor;
- 8.80.4. Deve ser composto por fibras ópticas tipo tight buffer (900µm) revestidas individualmente por material termoplástico e identificadas por cores;
- 8.80.5. Deve possuir proteção contra umidade através de materiais hidro expansíveis;
- 8.80.6. Deve possuir elementos de tração em fios de Aramida;
- 8.80.7. Deve possuir capa externa em material termoplásticos retardante à chama, resistente aos raios UV e com fio de rasgamento.
- 8.80.8. Deve atender aos requisitos da norma ABNT NBR 14772;
- 8.80.9. Deve possuir certificado de homologação da ANATEL;
- 8.80.10. Deve ser fornecidos os acessórios, kits de ancoragem e suspensão necessários para instalação;
- 8.80.11. Fornecimento de material para lubrificação do cabo e/ou dos dutos, conforme a necessidade.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.80.12. Fornecimento de prendedores e/ou fixadores, conforme a necessidade.
- 8.80.13. Serviço de lançamento do cabo, percorrendo toda a infraestrutura atendendo às recomendações do fabricante.
- 8.80.14. Os raios de curvatura dos cabos de fibra óptica instalados não poderão ser inferiores a 10 vezes seu diâmetro externo;
- 8.80.15. A tração máxima a ser imposta nos cabos de fibra óptica, durante a instalação, deverá ser de 1 x Peso do cabo por km;
- 8.80.16. Visando manter a integridade do cabeamento, suas pontas devem ser fechadas durante o lançamento.
- 8.80.17. Apresentar catálogo do fabricante

**8.81. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE CABO DE FIBRA ÓPTICA INDOOR/OUTDOOR 12FO MM 50/125 OM3**

- 8.81.1. A instalação de cabeamento óptico compreende os procedimentos necessários para instalação do metro de cabo de fibra óptica 12FO mm 50/125 OM3 interno ou externo, incluindo as seguintes atividades e materiais:
- 8.81.2. Fornecimento de cabo óptico 12 FO mm 50/125 OM3 interno ou externo, com as seguintes especificações:
- 8.81.3. Deve ser composto de 12 fibras ópticas e ser projetado para uso indoor/outdoor;
- 8.81.4. Deve ser composto por fibras ópticas tipo tight buffer (900µm) revestidas individualmente por material termoplástico e identificadas por cores;
- 8.81.5. Deve possuir proteção contra umidade através de materiais hidro expansíveis;
- 8.81.6. Deve possuir elementos de tração em fios de Aramida;
- 8.81.7. Deve possuir capa externa em material termoplásticos retardante à chama, resistente aos raios UV e com fio de rasgamento.
- 8.81.8. Deve atender aos requisitos da norma ABNT NBR 14772;
- 8.81.9. Deve possuir certificado de homologação da ANATEL;
- 8.81.10. Deve ser fornecido os acessórios, kits de ancoragem e suspensão necessários para instalação;
- 8.81.11. Fornecimento de material para lubrificação do cabo e/ou dos dutos, conforme a necessidade.
- 8.81.12. Fornecimento de prendedores e/ou fixadores, conforme a necessidade.
- 8.81.13. Serviço de lançamento do cabo, percorrendo toda a infraestrutura definida e atendendo às recomendações do fabricante.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.81.14. Os raios de curvatura dos cabos de fibra óptica instalados não poderão ser inferiores a 10 vezes seu diâmetro externo;
- 8.81.15. A tração máxima a ser imposta nos cabos de fibra óptica, durante a instalação, deverá ser de 1 x Peso do cabo por km;
- 8.81.16. Visando manter a integridade do cabeamento, suas pontas devem ser fechadas durante o lançamento.
- 8.81.17. Apresentar catálogo do fabricante.

**8.82. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE FIBRA ÓPTICA INDOOR/OUTDOOR 06FO SM**

- 8.82.1. A instalação de cabeamento óptico 06FO SM autossustentável compreende os procedimentos necessários para instalação do metro de cabo de fibra óptica, incluindo as seguintes atividades e materiais:
- 8.82.2. Fornecimento de cabo óptico 06FO SM autossustentável com as seguintes especificações:
- 8.82.3. Deve ser composto de 06 fibras ópticas e ser projetado para uso indoor/outdoor;
- 8.82.4. Deve ser composto por fibras ópticas tipo tight buffer (900µm) revestidas individualmente por material termoplástico e identificadas por cores;
- 8.82.5. Deve possuir proteção contra umidade através de materiais hidro expansíveis;
- 8.82.6. Deve possuir elementos de tração em fios de Aramida;
- 8.82.7. Deve possuir capa externa em material termoplásticos retardante à chama, resistente aos raios UV e com fio de rasgamento.
- 8.82.8. Deve atender aos requisitos da norma ABNT NBR 14772;
- 8.82.9. Deve possuir certificado de homologação da ANATEL;
- 8.82.10. Deve ser fornecidos os acessórios, kits de ancoragem e suspensão necessários para instalação;
- 8.82.11. Fornecimento de material para lubrificação do cabo e/ou dos dutos, conforme a necessidade.
- 8.82.12. Fornecimento de prendedores e/ou fixadores, conforme a necessidade.
- 8.82.13. Serviço de lançamento do cabo, percorrendo toda a infraestrutura atendendo às recomendações do fabricante.
- 8.82.14. Os raios de curvatura dos cabos de fibra óptica instalados não poderão ser inferiores a 10 vezes seu diâmetro externo;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.82.15. A tração máxima a ser imposta nos cabos de fibra óptica, durante a instalação, deverá ser de 1 x Peso do cabo por km;
- 8.82.16. Visando manter a integridade do cabeamento, suas pontas devem ser fechadas durante o lançamento.
- 8.82.17. Apresentar catálogo do fabricante.

**8.83. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE FIBRA ÓPTICA INDOOR/OUTDOOR 12FO SM**

- 8.83.1. A instalação de cabeamento óptico 12FO SM autossustentável compreende os procedimentos necessários para instalação do metro de cabo de fibra óptica, incluindo as seguintes atividades e materiais:
- 8.83.2. Fornecimento de cabo óptico 12FO SM autossustentável com as seguintes especificações:
- 8.83.3. Deve ser composto de 12 fibras ópticas e ser projetado para uso indoor/outdoor;
- 8.83.4. Deve ser composto por fibras ópticas tipo tight buffer (900µm) revestidas individualmente por material termoplástico e identificadas por cores;
- 8.83.5. Deve possuir proteção contra umidade através de materiais hidro expansíveis;
- 8.83.6. Deve possuir elementos de tração em fios de Aramida;
- 8.83.7. Deve possuir capa externa em material termoplásticos retardante à chama, resistente aos raios UV e com fio de rasgamento.
- 8.83.8. Deve atender aos requisitos da norma ABNT NBR 14772;
- 8.83.9. Deve possuir certificado de homologação da ANATEL;
- 8.83.10. Deve ser fornecido os acessórios, kits de ancoragem e suspensão necessários para instalação;
- 8.83.11. Fornecimento de material para lubrificação do cabo e/ou dos dutos, conforme a necessidade.
- 8.83.12. Fornecimento de prendedores e/ou fixadores, conforme a necessidade.
- 8.83.13. Serviço de lançamento do cabo, percorrendo toda a infraestrutura definida e atendendo às recomendações do fabricante.
- 8.83.14. Os raios de curvatura dos cabos de fibra óptica instalados não poderão ser inferiores a 10 vezes seu diâmetro externo;
- 8.83.15. A tração máxima a ser imposta nos cabos de fibra óptica, durante a instalação, deverá ser de 1 x Peso do cabo por km;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

8.83.16. Visando manter a integridade do cabeamento, suas pontas devem ser fechadas durante o lançamento.

8.83.17. Apresentar catálogo do fabricante.

**8.84. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD ÓPTICO DUPLEX LC-LC MM 50/125 - OM3 DE 2,5 A 5 MTS**

8.84.1. A instalação com fornecimento de patch cord de fibra óptica duplex LC-LC MM 50/125 - OM3 DE 2,5 A 5 mts compreende os procedimentos necessários para disponibilizar o link de dados, incluindo as seguintes atividades e materiais:

8.84.2. Fornecimento de patch cord duplex LC-LC MM 50/125 - OM3 DE 2,5 A 5 mts com as seguintes especificações:

8.84.3. A perda máxima por inserção deve ser de 0.25 dB.

8.84.4. A perda mínima por retorno deve ser de 26dB.

8.84.5. Deve ter comprimento de 2,5m a 5m.

8.84.6. Classe de flamabilidade LSZH.

8.84.7. A fibra deve ser multimodo, OM3, de índice gradual com especificações de 50/125mm e devendo suportar velocidades de transmissão de até 10 Gbits/seg, para comprimentos de até 300 metros com comprimentos de onda de 850 nm para a IEEE802.3ae.

8.84.8. Devem estar em conformidade com as normas ISO/IEC 11801, TIA/EIA-568-C.3, TIA-604-3 (FOCIS-3), TIA-604-10 (FOCIS-10).

8.84.9. Os conectores devem suportar no mínimo 500 ciclos de inserção.

8.84.10. Os conectores devem ser do tipo SFF (LC) duplex em ambas as extremidades;

8.84.11. O serviço de instalação deve ser realizado com cautela, visando garantir a integridade dos cabos ópticos existentes.

8.84.12. Apresentar catálogo do fabricante;

**8.85. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PATCH CORD ÓPTICO DUPLEX LC-LC SM DE 2,5 A 5 MTS**

8.85.1. A instalação com fornecimento de patch cord duplex LC-LC SM de 2,5 A 5 mts de fibra óptica compreende os procedimentos necessários para disponibilizar o link de dados, incluindo as seguintes atividades e materiais:

8.85.2. Fornecimento de patch cord duplex LC-LC SM de 2,5 A 5 mts com as seguintes especificações:

8.85.3. A perda por máxima por inserção deve ser de 0.35 dB;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.85.4. A perda mínima por retorno deve ser de 55dB;
- 8.85.5. Deve ter comprimento de 2,5m a 5m;
- 8.85.6. Classe de flamabilidade LSZH;
- 8.85.7. A fibra deve ser multimodo, OS1 ou OS2, de índice gradual com especificações de 9/125mm;
- 8.85.8. Devem estar em conformidade com as normas ISO/IEC 11801, TIA/EIA-568-C.3, TIA-604-3 (FOCIS-3), TIA-604-10 (FOCIS-10);
- 8.85.9. Os conectores devem suportar no mínimo 500 ciclos de inserção;
- 8.85.10. Os conectores devem ser do tipo SFF (LC) duplex em ambas as extremidades;
- 8.85.11. O serviço de instalação deve ser realizado com cautela, visando garantir a integridade dos cabos ópticos existentes.
- 8.85.12. Apresentar catálogo do fabricante

**8.86. SERVIÇO DE FUSÃO DE FIBRA ÓPTICA**

- 8.86.1. As emendas ópticas deverão ser realizadas dentro das caixas de emendas ou distribuidores ópticos internos e deverão ser feitas de modo a evitar que as mesmas sejam submetidas a qualquer esforço mecânico;
- 8.86.2. Todas as emendas deverão ser realizadas através do processo de fusão usando equipamento de fusão óptica com alinhamento pelo núcleo, protegidas por meio de tubetes termocontráteis. A atenuação máxima por emenda não poderá exceder 0,05dB;
- 8.86.3. Abertura e fechamento de DIO ou Caixa de Emenda óptica em local aéreo ou subterrâneo;
- 8.86.4. Acomodação dos protetores de emenda (tubetes) na bandeja;
- 8.86.5. Emissão do relatório impresso ou meio eletrônico no formato PDF das fusões realizadas.
- 8.86.6. A máquina usada para realizar as fusões ópticas deverá ter processo automático, com interrupção do processo, caso detecte erro na clivagem ou sujeira na fibra. A máquina deverá realizar inspeção automática da fibra antes e depois da emenda.
- 8.86.7. Deverá ser utilizada etiqueta de identificação legível para o DIO ou Caixa de Emenda Óptica após as fusões, com impressora etiquetadora, fita duradoura (não descolar ou desprender facilmente) e práticas (facilitar a manutenção e visualização);
- 8.86.8. A unidade utilizada para medir esse serviço é a própria fusão.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

**8.87. SERVIÇO CERTIFICAÇÃO DE FIBRA ÓPTICA**

- 8.87.1. A certificação de enlace óptico utilizando OTDR: Reflectômetro Óptico no Domínio do Tempo.
- 8.87.2. O equipamento OTDR deve verificar:
- 8.87.3. Uniformidade de atenuação óptica;
- 8.87.4. Picos de Fresnel;
- 8.87.5. Perda nas emendas;
- 8.87.6. Perda nos conectores;
- 8.87.7. Atenuação da fibra óptica;
- 8.87.8. Distância dos lances de cabos;
- 8.87.9. Comprimento de enlace óptico.
- 8.87.10. O equipamento deverá funcionar com os seguintes comprimentos de onda:
- 8.87.11. Monomodo
- 8.87.12. 1310 nm +/- 25 nm
- 8.87.13. 1550 nm +/- 30 nm
- 8.87.14. O equipamento deverá funcionar com os seguintes tipos de fibra compatíveis:
- 8.87.15. Monomodo: 9/125 µm
- 8.87.16. O equipamento deverá funcionar as distâncias máximas:
- 8.87.17. Monomodo - 130 km
- 8.87.18. As certificações com o OTDR devem ser feitas nos dois sentidos para eliminar erros inerentes à técnica de reflectometria óptica.
- 8.87.19. Deverá ser entregue laudo impresso dos testes com os gráficos e resultados.
- 8.87.20. O resultado esperado da certificação é um relatório, que deverá ser entregue impresso ou meio eletrônico em formato PDF. Esse relatório deverá agrupar os enlaces certificados por trecho.

**8.88. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE PONTOS DE ENERGIA**

- 8.88.1. Compreende os passos necessários para a instalação de 2 tomadas elétricas estabilizadas modelo 2P+T padrão NBR em cada área de trabalho, abrangendo as

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
seguintes atividades e materiais:

- 8.88.2. Fornecimento e instalação de 90 metros de fio 2,5mm, sendo 3 segmentos de cada uma das cores definidas para cada circuito elétrico com as seguintes especificações:
- 8.88.3. Formado por fios de cobre eletrolítico nu, têmpera mole e encordoamento classe 4;
- 8.88.4. Suporte a tensão nominal de 450/750V;
- 8.88.5. Antichama com isolamento em PVC/A para 70°C;
- 8.88.6. Aprovado e certificado pelo INMETRO;
- 8.88.7. Fornecimento e instalação de 2 tomadas 2P+T compatível com espelho e caixa para canaleta;
- 8.88.8. Fornecimento e instalação de terminadores de fio;
- 8.88.9. Realização das conexões em disjuntores;
- 8.88.10. Realização de testes e medições;
- 8.88.11. Identificação dos fios, circuitos e tomadas.
- 8.88.12. Apresentar catálogo do fabricante;

**8.89. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE QUADRO DE DISTRIBUIÇÃO ELÉTRICO PARA ATE 28 DISJUNTORES**

- 8.89.1. Compreende os passos e fornecimentos necessários para disponibilizar a instalação de disjuntores e sistemas de proteção de energia, para a adequada segmentação dos circuitos elétricos, incluindo as seguintes atividades e materiais:
- 8.89.2. Instalar o quadro em local apropriado com as seguintes especificações:
- 8.89.3. Construído em material metálico;
- 8.89.4. Tipo sobrepor;
- 8.89.5. Capacidade mínima de disjuntores conforme especificado no respectivo item;
- 8.89.6. Equipado com barramento de cobre com as seguintes especificações:
- 8.89.7. Pureza de 99%;
- 8.89.8. Trifásico;
- 8.89.9. Tipo DIN;
- 8.89.10. Interligar com o aterramento pré-existente saindo do barramento geral, máximo

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

de 50m;

- 8.89.11. Deverão ser fornecidos parafusos com buchas, fazer marcação de furos e fazer furos em paredes;
- 8.89.12. Deverão ser fornecidos dois disjuntores trifásicos tipo DIN 63A e 28 disjuntores DIN monofásicos 16A com as seguintes especificações:
- 8.89.13. Tipo DIN;
- 8.89.14. Capacidade de interrupção (Icn) mínima de 5 kA 127/230 V - 3 kA 230/400 V, Curva C;
- 8.89.15. Temperatura de operação entre -5° C a +60° C.
- 8.89.16. Deverão ser fornecidos 04 dispositivos protetores de surto monopolares, sendo 03 para as fases e 01 para o neutro, com as seguintes características:
- 8.89.17. Monopolar;
- 8.89.18. Capacidade mínima de corrente de descarga conforme especificado no respectivo item;
- 8.89.19. Suporte às tensões F / N 230 V, 50/60 Hz e F / F 400 V, 50/60 Hz;
- 8.89.20. Grau de proteção IP20;
- 8.89.21. Temperatura de operação entre -5° C a +60° C.
- 8.89.22. A instalação deve estar em conformidade com as especificações previstas na NBR 5410 (norma que regulamenta as instalações elétricas em baixa tensão) e NR-10 (segurança em instalações e serviços em eletricidade).
- 8.89.23. Serviço de identificação do circuito;
- 8.89.24. Apresentar catálogo do fabricante;

**8.90. SERVIÇO DE INTERLIGAÇÃO DE QUADRO ELÉTRICO TRIFÁSICO AO QUADRO GERAL ATÉ 60MTS**

- 8.90.1. Consiste em lançar 5 cabos, neutro / aterramento / fase / fase / fase, do quadro instalado até o quadro geral do edifício com as seguintes especificações:
- 8.90.2. Seção nominal 25mm<sup>2</sup>;
- 8.90.3. Formado por fios de cobre eletrolítico, têmpera mole e encordoamento classe 5;
- 8.90.4. Suporte a tensão nominal de 0,6/1KV;
- 8.90.5. Antichama com isolamento em PVC/A para 70°C;

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 8.90.6. A cobertura do cabo deverá ser PVC/ST1;
- 8.90.7. Aprovado e certificado pelo INMETRO.
- 8.90.8. Fornecimento dos acessórios necessários à realização das conexões nas extremidades, tais como: conectores e terminais de compressão (em cobre estanhado), parafusos, porcas e arruelas em aço inox.
- 8.90.9. Serviço de lançamento do cabo, percorrendo toda a infraestrutura atendendo às recomendações do fabricante.
- 8.90.10. Serviço de instalação do cabo, conectorizando-o atendendo às recomendações do fabricante.
- 8.90.11. A instalação deve estar em conformidade com as especificações previstas na NBR 5410 (norma que regulamenta as instalações elétricas em baixa tensão) e NR-10 (segurança em instalações e serviços em eletricidade).
- 8.90.12. Serviço de identificação do circuito;
- 8.90.13. Apresentar catálogo do fabricante;

**8.91. SERVIÇO DE INSTALAÇÃO COM FORNECIMENTO DE ATERRAMENTO BÁSICO.**

- 8.91.1. A instalação de aterramento básico compreende os procedimentos necessários para proteção de racks ou quadros elétricos, incluindo as seguintes atividades e materiais:
- 8.91.2. Fornecimento de 05 barras de terra 5/8" x 2,4m;
- 8.91.3. Fornecimento de cabo de cobre nu 25mm<sup>2</sup>;
- 8.91.4. Fornecimento de caixa de inspeção para aterramento;
- 8.91.5. Serviço de instalação das barras de terra em conformidade com as normas técnicas vigentes;
- 8.91.6. Serviço de interligação do sistema básico de aterramento ao quadro elétrico ou rack;
- 8.91.7. Serviço de instalação do cabo de cobre;
- 8.91.8. Serviço de instalação da caixa de inspeção para aterramento.

**8.92. SERVIÇO DE REMANEJAMENTO DE PONTO LÓGICO OU ELÉTRICO, SEM FORNECIMENTO DE MATERIAIS E INFRA ESTRUTURA**

- 8.92.1. O remanejamento de ponto lógico ou elétrico consiste em efetuar o remanejamento do conjunto físico da rede em infraestrutura existente, que compreende conectores, tomadas, caixa de tomadas, espelhos e patch cord's, devendo ser observado as melhores práticas de encaminhamento tais como evitar contato com cabos elétricos, curvaturas etc. Compreende os procedimentos

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
necessários para mudar a posição de um ponto existente, incluindo as seguintes atividades:

- 8.92.2. Fornecimento de materiais de acabamento, conforme a superfície perfurada (massa, gesso, cimento, selador e tinta).
- 8.92.3. Fornecimento de parafusos com buchas, conforme a superfície existente (alvenaria, gesso, divisória, drywall, madeira).
- 8.92.4. Serviço de desprendimento e remoção de canaleta e respectivos acessórios.
- 8.92.5. Serviço de fixação de canaleta e respectivos acessórios.
- 8.92.6. Serviço de recorte de canaleta.
- 8.92.7. Serviço de desprendimento e remoção de caixa de superfície e respectivos acessórios.
- 8.92.8. Serviço de fixação de caixa de superfície e respectivos acessórios.
- 8.92.9. Serviço de decomposição e recomposição do espelho com as tampas cegas.
- 8.92.10. Serviço de desconexão do cabo de seu respectivo conector.
- 8.92.11. Serviço de retirada de cabo lógico ou elétrico de suas respectivas infraestruturas, dentre as quais: canaletas, eletrodutos, eletrocalhas, mangueiras, Seal tubes.
- 8.92.12. Serviço de lançamento de cabo lógico ou elétrico, percorrendo toda a infraestrutura.
- 8.92.13. Serviço de crimpagem do conector RJ45 ao cabo.
- 8.92.14. Serviço de conectorização da tomada elétrica e aos cabos.

### **8.93. SERVIÇO DE ELABORAÇÃO DE AS-BUILT**

- 8.93.1. Fornecimento de mão-de-obra especializada para a atualização de projeto executivo, "As-Built".
- 8.93.2. A Documentação Técnica de alterações e novas instalações deverá conter todas as informações necessárias do parque instalado da respectiva rede, e contemplar informações sobre todos os pontos da rede de cabeamento estruturado atualizado ou a rede de fibra óptica atualizado, ou rede elétrica atualizada, etc, e identificar cada ponto da rede de cabeamento estruturado, ou rede fibra óptica ou rede elétrica, ou outro, com diagrama geral da rede identificando as caixas de passagem, ou racks, e pontos e outros. O software empregado na confecção dos textos integrantes da documentação técnica deverá ser no formato Open Document (.odt), ou outro compatível, o software empregado na confecção dos desenhos integrantes da documentação técnica deverá ser o AUTOCAD, versão 2010 ou superior;
- 8.93.3. O resultado esperado do projeto executivo é um documento atualizado "As Built",

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
impresso e em arquivo digital;

- 8.93.4. Deverá ser anexada ao As-Built a certificação de todo cabeamento óptico instalado, ou cabeamento UTP, ou elétrico com identificação da rede.
- 8.93.5. A unidade utilizada para medir esse serviço é o projeto executivo atualizado em si, mediante dados dos serviços executados atualizando o projeto original. Assim, cada projeto que será entregue deve ter um valor a ser pago, independentemente da quantidade de profissionais e de horas requeridas para a realização da visita ou projeto;

#### **8.94. TREINAMENTO/REPASSE DE CONHECIMENTO**

- 8.94.1. O treinamento deverá ocorrer conforme plano de capacitação, podendo ser realizado nas dependências da CONTRATANTE ou de forma ONLINE.
- 8.94.2. Deverá constar no plano de capacitação o cronograma e ementa do conteúdo a ser ministrado.
- 8.94.3. O plano de capacitação deverá abordar todas a solução definida nesta especificação.
- 8.94.4. A CONTRATADA deverá disponibilizar de forma local ou remota, instrutor devidamente capacitado na solução ofertada, às expensas da CONTRATADA, para efetuar o treinamento para até 05 (cinco) técnicos da Contratante, simultaneamente, com material didático.;
- 8.94.5. É permitido à CONTRATADA subcontratar, sob sua inteira responsabilidade, instrutor devidamente capacitado na solução ofertada para ministrar o treinamento.
- 8.94.6. O treinamento deve ser ministrado em português do Brasil. O material do treinamento deve ser, preferencialmente, em português. Caso não exista material do produto em português, será aceito material em inglês.

#### **9. HOMOLOGAÇÃO TÉCNICA**

- 9.1. A homologação será realizada em uma única etapa. No momento da homologação será efetuada a verificação dos catálogos/manuais oficiais dos produtos ofertados, com atendimento das características técnicas requeridas e demais documento técnicos como atendimento aos requisitos da qualificação técnica.
- 9.2. Ao não atendimento de qualquer dos requisitos técnicos e suas respectivas documentações, a empresa será desclassificada.

#### **10. SLA – ACORDO DE NÍVEL DE SERVIÇO**

- 10.1. O Acordo de Nível de Serviços (SLA) são especificados para a gestão de infraestrutura, abrangendo todos os prazos e ações acordadas para uma boa execução contratual.
- 10.2. O estabelecimento de SLAs objetiva estabelecer responsabilidades claras para a CONTRATADA, a fim de permitir o acompanhamento do seu desempenho, de forma a

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

assegurar que os níveis de serviços definidos sejam continuamente mantidos e aprimorados.

**10.2.1. SLA – OPERAÇÃO E MANUTENÇÃO DURANTE A GARANTIA;**

REQUISITOS OBRIGATÓRIOS	REFERÊNCIA
<b>Ativação/Entrega</b> – Período entre a solicitação e entrega.	90 (noventa) dias, prorrogável por igual período desde que devidamente justificado.
<b>Prazo de atendimento</b> – Período máximo para atendimento e identificação do problema, contado a partir do momento da abertura do chamado até a finalização do atendimento.	4 (quatro) horas
<b>Abertura de Chamado</b> – Disponibilidade de atendimento para solicitações de reparos.	24 x 7 (00:00 às 24:00 de Segunda a Domingo)
<b>Horário de Reparo</b> – Disponibilidade de atendimento técnico a partir da abertura da chamada.	24 x 7 (00:00 às 24:00 de Segunda a Domingo)
<b>Substituição de Peças</b> – Prazo para substituição de peças defeituosas, não disponíveis no local, durante a vigência contratual.	NBD - Próximo dia útil.(envio de peça com chegada no local no próximo dia útil)

**11. SERVIÇO SUPORTE E ATENDIMENTO**

11.1. A CONTRATADA deverá manter um canal de atendimento gratuito, de central acionada por meio de ligação gratuita, ou ligação local, ou e-mail, ou abertura de chamado em portal de atendimento da CONTRATADA para suporte técnico e solicitações de baixa complexidade disponível 24 x 7 (00:00 às 24:00 de Segunda a Domingo).

**11.2. ATENDIMENTO TÉCNICO À DISTÂNCIA**

11.2.1. A CONTRATADA deverá permitir o registro de solicitações de atendimento técnico à distância, em regime de garantia.

11.2.2. Entende-se por suporte técnico à distância a execução, por telefone, e-mail ou acesso remoto de procedimentos destinados a esclarecer dúvidas, orientar a execução de configurações, aplicar atualizações de software remotamente, auxiliar na administração da solução e quaisquer outros que tenham por objetivo ajudar a CONTRATANTE a melhor utilizar a solução e caso seja possível, efetuar qualquer manutenção corretiva.

11.2.3. As solicitações de atendimento técnico à distância partirão da gestão ou fiscalização contratual e deverão ser lançadas em registro próprio pela CONTRATADA.

11.2.4. Para cada solicitação de atendimento técnico à distância, deverá ser gerado um identificador único e sequencial para fins de controle e acompanhamento da solicitação.

11.2.5. A CONTRATADA deverá prestar atendimento técnico à distância, em regime de garantia e suporte.

11.2.6. O atendimento técnico à distância poderá envolver manutenção preventiva ou corretiva, sem ônus adicional à CONTRATANTE.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 11.2.7. Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar a solução em seu perfeito estado de uso.
- 11.2.8. Entende-se por término de reparo a disponibilidade da solução para uso em perfeitas condições de funcionamento, no local onde estiver instalado, atestado pela CONTRATANTE.
- 11.2.9. Ao final de cada atendimento técnico à distância, a CONTRATADA deverá apresentar “Relatório de Atendimento” ou documento similar, contendo a data, hora de chamada, início e término do atendimento, identificação do problema, providências adotadas e outras informações que sejam pertinentes, a ser assinada pela CONTRATANTE e pelo responsável pela manutenção.
- 11.2.10. A CONTRATADA deverá prestar atendimento técnico à distância, por técnicos devidamente habilitados.

## **12. DA VISTORIA**

- 12.1. As empresas interessadas em fornecer os produtos/serviços poderão realizar vistoria técnica prévia, com a finalidade de conhecer o local onde deverão ser executados os serviços e inteirar-se das condições e grau de dificuldade existentes, e para obtenção de todas as informações necessárias à correta elaboração da proposta.
- 12.2. A vistoria visa afastar futuras alegações de desconhecimento e/ou de dificuldades na execução dos serviços, e por ocasião de sua realização, será emitido uma Declaração de Vistoria Técnica, assinado pelo representante da proponente e por servidor da CONTRATANTE da área técnica demandante.
- 12.3. A vistoria será agendada para todas as empresas interessadas, com antecedência mínima de 48 horas, mediante contato com a Diretoria Tecnologia da Informação, pelo e-mail: [diretoria.dti@tcm.pa.gov.br](mailto:diretoria.dti@tcm.pa.gov.br), até o 2º (segundo) dia útil anterior à data de abertura do certame.
- 12.4. A vistoria deverá ser realizada pelos responsáveis técnicos ou por representante legal da licitante, acompanhado por técnico da CONTRATANTE, até o 1º dia útil que anteceder a data de abertura da licitação, no horário de 8:00h às 15:00h, de segunda a sexta-feira.
- 12.5. Após a vistoria, a CONTRATANTE fornecerá declaração de que a licitante se encontra ciente e de acordo com as condições do serviço a ser executado e especificações do material a ser fornecido.
- 12.6. Por ocasião da vistoria, a licitante não poderá alegar, posteriormente, desconhecimento de quaisquer necessidades para a execução dos respectivos serviços a serem realizados e dos aspectos técnicos a serem considerados em sua execução nas características, exigências e competências descritas nesta especificação.
- 12.7. O proponente optando por não realizar a vistoria, deverá apresentar Termo de Abstenção de vistoria e não poderá alegar desconhecimento ou se eximir da responsabilidade na ocorrência de eventuais dificuldades, custos adicionais ou prejuízos que poderiam ter sido previstos por vistoria prévia, mediante a falta da vistoria.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

**13. DA PARTICIPAÇÃO DE ME E EPP**

- 13.1. Justifica-se a não reserva de cotas nos termos estabelecidos nos art. 47 e 48 da Lei Complementar n.º 123/2006 alterada pela Lei Complementar n.º 147/2014, visto se tratar de contratação de bens de natureza não divisível, de acordo com o justificado neste Termo de Referência.
- 13.2. Considerando que o valor referencial obtido por meio da coleta de orçamentos, foi superior a R\$-80.000,00 (oitenta mil reais), aplicar-se-á tão somente a preferência a MEs/EPPs no caso de empate ficto, em conformidade com os artigos 44 e 45 da LC n.º 123/2006.

**DOS CRITÉRIOS DE ELABORAÇÃO DA PROPOSTA COMERCIAL VENCEDORA DOS LANCES**

- 14.1. A proposta vencedora dos lances deverá apresentar as seguintes condições:
- 14.2. Prazo de validade, não inferior a 60 (sessenta) dias, a contar da data de sua apresentação;
- 14.3. Preço total da solução proposta, de acordo com os preços praticados no mercado, conforme estabelece o art. 43, inciso IV, da Lei no 8.666/93, em algarismo e por extenso, expresso em moeda corrente nacional (R\$), considerando as especificações constantes do Termo de Referência;
- 14.4. Estarem incluídos no preço todos os insumos que o compõe, tais como, as despesas com mão de obra, impostos, taxas, frete, seguros e quaisquer outros que incidam direta ou indiretamente no fornecimento do objeto desta licitação;
- 14.5. Conter indicação de marca e modelo, *part number*, para todos os produtos de forma a demonstrar cumprimento das exigências consignadas no Termo de Referência, e para os serviços, identificar as características dos mesmos.
- 14.6. Atender as condições complementares constantes deste Termo de Referência.
- 14.7. Especificações técnicas completas dos serviços a serem fornecidos, sendo desconsiderada a proposta da licitante que deixar de apresentar, ou apresentar em discordância com as especificações do presente Termo de Referência, Anexos/Apêndices e nos termos abaixo:
- 14.8. Descrever individualmente e com clareza marca, modelo, *part number*, quantidades e outras informações aplicáveis e necessárias à perfeita caracterização dos itens propostos de acordo com as características solicitadas no Termo de Referência;
- 14.9. Deve conter todas as informações da proponente: razão social, CNPJ, endereço, telefone, e-mail, dados bancários, sócios administradores, e respectiva qualificação deles (nome, endereço, CPF, RG, e-mail, telefone de contato, cargo na empresa) e assinatura do representante legal .
- 14.10. Declarar que os preços contemplam todas as despesas/custos, materiais, ferramentas impostos, mão de obra, etc., necessárias a entrega dos itens (produtos ou serviços);

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

**15. DO PRAZO DE ENTREGA / EXECUÇÃO**

- 15.1. A CONTRATADA fica obrigada a entregar os equipamentos em até 90 (noventa) dias após a assinatura do contrato.
- 15.2. A execução dos serviços correrá em até 90 (noventa) dias após o devido recebimento definitivo dos equipamentos e mediante ordem de serviço.
- 15.3. Em caso de necessidade de prorrogação do prazo, a CONTRATADA deverá proceder solicitação formal e fundamentada à CONTRATANTE.

**16. DA ENTREGA E DO RECEBIMENTO DO OBJETO**

- 16.1. A entrega deverá ocorrer no horário de 8:00 às 15:00 horas, de segunda a sexta-feira, exceto feriados, na sede da CONTRATANTE, ou em horário diverso para fins de minimizar impacto nas atividades da CONTRATANTE, devendo ser acordado entre as partes.
- 16.2. Os bens/produtos/serviços/ software serão recebidos, provisoriamente, no ato de entrega, para efeito de posterior verificação da conformidade com as especificações constantes do Termo de Referência.
- 16.3. Os bens/produtos/serviços/ software serão recebidos, definitivamente, em no máximo 15 (quinze) dias contados a partir da entrega ou instalação dos bens/produtos/serviços/software, devendo o(s) fiscal(is) ou responsável(is) designado(s) terem procedido, neste interregno, a verificação da qualidade, testes e outros, dos bens/produtos/serviços/software disponibilizados. Mediante sua aceitação será procedido a emissão de Termo de Recebimento Definitivo assinado pelo(s) responsável(eis) da CONTRATANTE.
- 16.4. A CONTRATANTE deverá convocar a CONTRATADA para acompanhamento e realização dos testes a serem realizados dentro do prazo estabelecido.
- 16.5. Caso ocorram problemas durante a execução desta etapa, a CONTRATANTE apontará por escrito as razões para deixar de emitir o Termo de Recebimento Definitivo e indicará as falhas ou pendências verificadas à CONTRATADA, a qual deverá providenciar sua correção ou substituição, arcando com o ônus decorrente.
- 16.6. Os serviços somente serão considerados aceitos depois de minucioso teste de funcionamento efetuado, dentro do prazo de 15 dias estabelecido acima, pela equipe de técnicos da CONTRATANTE e da CONTRATADA. Tais testes visam à checagem das perfeitas condições físicas, funcionamento e atendimento às especificações em conformidade com os Requisitos Técnicos descritos neste Termo de Referência.
- 16.7. Ocorrendo qualquer problema ou divergência nos testes, a Contratada terá o prazo de até 10 (dez) dias úteis, contados a partir da notificação, para proceder às correções, adequações ou substituição do item, objeto deste ajuste, voltando a proceder os testes de aceitabilidade definitiva conforme disposto.
- 16.8. Caso a correção dos desvios/ defeitos/ não sejam atendimentos no período de até 10 (dez) dias úteis, contados a partir da data da primeira notificação, a contagem do prazo

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

de notificação para correção dos desvios constatados não será interrompida devido à rejeição deles. Neste caso, a Contratada arcará com o ônus decorrente desse atraso.

- 16.9. Uma vez constatado o funcionamento do objeto entregue com os termos contratuais, a CONTRATANTE efetuará o recebimento definitivo do objeto contratado.
- 16.10. O aceite e o posterior pagamento dos produtos não eximem a licitante vencedora das responsabilidades pela correção de todos os defeitos, falhas e quaisquer outras irregularidades decorrentes dos produtos aplicados e dos serviços prestados nos termos da garantia.
- 16.11. O recebimento definitivo caberá ao agente fiscalizador especialmente designado para o acompanhamento e a fiscalização do contrato decorrente desta proposição.
- 16.12. Ficam designados para compor a comissão que efetuará o recebimento definitivo, o agente fiscalizador e o gestor do contrato, bem como, seus respectivos substitutos.

**17. LOCAL DE ENTREGA E EXECUÇÃO DOS OBJETO**

- 17.1. A entrega deverá ocorrer no horário de 8:00 às 15:00 horas, de segunda a sexta-feira, exceto feriados, na sede da CONTRATANTE, ou em horário diverso para fins de minimizar impacto nas atividades da CONTRATANTE, devendo ser acordado entre as partes.
- 17.2. A execução deverá ocorrer no local contratado e preferencialmente em horário comercial, podendo ocorrer em outros horários pré-definidos entre CONTRATANTE e CONTRATADA, conforme a natureza dos serviços em caso de necessidade, para fins minimizar impacto nas atividades da CONTRATANTE.

**18. PRAZO DE VIGÊNCIA E EXECUÇÃO DO CONTRATO**

- 18.1. O prazo de duração do presente ajuste administrativo será de 12 (doze) meses, a contar da data da sua assinatura, podendo ser prorrogado, observado o prazo máximo de 60 (sessenta) meses, em conformidade com a permissibilidade legal, em obediência ao previsto no inciso II do art. 57 da Lei Federal n.º 8.666/93 e alterações.
- 18.2. A CONTRATADA deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do art. 65 da Lei Federal n.º 8.666/93

**19. MEIOS FORMAIS DE COMUNICAÇÃO**

**19.1. COMUNICAÇÃO ENTRE CONTRATANTE E CONTRATADA**

- 19.1.1. A CONTRATADA junto com a CONTRATANTE deverá promover reuniões de acordo com as demandas em andamento no intuito de avaliar e zelar pela qualidade de atendimento e serviços.
- 19.1.2. A CONTRATADA deverá informar e-mail oficial para comunicações com a CONTRATANTE.
- 19.1.3. A CONTRATADA deverá informar número telefônico e contato técnico para comunicação ágil das atividades objeto desta especificação técnica.

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

- 19.1.4. Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

**20. SUBCONTRATAÇÃO**

- 20.1. Será admitida a subcontratação parcial do objeto, limitando-se nos serviços acessórios, complementares a exemplo de instalações de dutos, perfurações de paredes, recomposição de paredes, treinamento entre outros complementares. No entanto, a CONTRATADA será a única e exclusiva responsável pela execução do objeto ofertado, não tendo a SUBCONTRATADA qualquer vínculo com a CONTRATANTE.
- 20.2. A CONTRATADA, nas hipóteses de subcontratação, deverá de modo prévio e formal comunicar a CONTRATANTE, prestando-lhe todas as informações necessárias quanto aos sérvios que serão executados e a empresa subcontratada.

**21. DO VÍNCULO EMPREGATÍCIO**

- 21.1. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta, e não há dedicação de mão de obra exclusiva.
- 21.2. Os profissionais e representantes da CONTRATADA não terão nenhum vínculo empregatício com a CONTRATANTE, correndo por conta exclusiva da CONTRATADA, todas as obrigações decorrentes da legislação trabalhista, previdenciária, infortunistica do trabalho, fiscal, comercial e outras correlatas, as quais a CONTRATADA se obriga a saldar na época devida.

**22. DA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO**

- 22.1. A divisão da solução não é tecnicamente viável e existem fornecedores para toda a solução, não sendo necessário, portanto, a aceitação da participação de consórcios.

**23. DAS OBRIGAÇÕES DA CONTRATANTE**

- 23.1. O TCMPA terá plenos poderes para fiscalizar e acompanhar a execução dos serviços por si ou por intermédio de prepostos devidamente credenciados, nas formas previstas na Lei 8.666/93.
- 23.2. Permitir o acesso dos funcionários ou prepostos da CONTRATADA às dependências da CONTRATANTE, respeitando as normas que disciplinam a segurança do patrimônio, das pessoas e das informações e os termos deste Termo de Referência;
- 23.3. Efetuar pagamento nos prazos e condições estabelecidos no contrato, conforme este Termo de Referência.
- 23.4. Apresentar na reunião de início do projeto os líderes das tecnologias que estarão envolvidos na implantação dos itens.
- 23.5. Fornecer as informações necessárias e de suas responsabilidades para fins de cumprimento do pactuado.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 23.6. Sugerir com a CONTRATADA o cronograma de atividades para alcançar a finalização do contratado no prazo mais exíguo possível e com menor impacto possível no andamento das rotinas de trabalho da CONTRATANTE.
- 23.7. Informar e diferenciar as informações que são sigilosas previamente ao seu fornecimento.
- 23.8. Garantir que as atualizações e adequações no ambiente da CONTRATANTE serão executadas, desde que adequadamente solicitado e justificado.
- 23.9. Todo trabalho será feito no termos definidos no Termo de Referência, o qual traz os quesitos técnicos norteadores do contrato por escrito, entre a CONTRATADA e o CONTRATANTE.

#### **24. DAS OBRIGAÇÕES DA CONTRATADA**

- 24.1. Apresentar na reunião de início da execução do contrato o nome, telefone e e-mail de um ponto de contato único através do qual poderá ser encaminhada e acompanhada qualquer pendência operacional ou administrativa.
- 24.2. Realizar a entrega dos itens atendendo aos requisitos técnicos exigidos em Termo de Referência;
- 24.3. Realizar os serviços contratados de instalação nos termos escritos no Termo de Referência.
- 24.4. Aplicar as normas técnicas vigentes aos serviços pactuados.
- 24.5. Disponibilização da documentação dos serviços prestados tais como: manuais de operação dos equipamentos e softwares, documentação das rotinas operacionais necessárias ao funcionamento da solução, descrição de problemas mais comuns e respectivas soluções.
- 24.6. Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências do CONTRATANTE.
- 24.7. Prestar toda a orientação necessária para instalação e a perfeita utilização dos materiais e sua aplicação para a obtenção de seu máximo desempenho.
- 24.8. Responsabilizar-se integralmente pelo fornecimento de mão-de-obra especializada com experiência comprovada na prestação de serviços similares e de igual porte.
- 24.9. Observar e adotar todas as recomendações dos fabricantes, devendo prever e incluir em sua proposta todos os elementos necessários ao seu correto e pleno funcionamento.
- 24.10. Responder por qualquer prejuízo que seus empregados ou preposto causarem ao patrimônio da CONTRATANTE, ou a terceiros, decorrentes de ação ou omissão culposa ou dolosa, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus decorrente.
- 24.11. Assumir total responsabilidade pelo sigilo das informações, classificadas como

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

sigilosas, que seus empregados ou prepostos vierem a obter em função dos serviços prestados, respondendo pelos danos causados a CONTRATANTE ou a terceiros em virtude de um eventual vazamento de informação, decorrente de ação dolosa, negligência, imperícia ou imprudência.

- 24.12. Manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos, framework e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revelá-los, divulga-los, reproduzi-los na sua totalidade ou em partes, ou deles dar conhecimento a quaisquer terceiros.
- 24.13. Comunicar previamente a CONTRATANTE, a necessidade da divulgação das INFORMAÇÕES CONFIDENCIAIS a que tenha tido acesso, devido a determinação judicial ou a ordem emanada por autoridade competente.
- 24.14. Por ocasião do encerramento do contrato, devolver a CONTRATANTE, toda e qualquer informação considerada confidencial e disponibilizada na forma de relatórios, arquivos, imagens, audiovisuais, ou quaisquer outros meios de armazenamento, comprometendo-se a removê-las de seus equipamentos servidores, microcomputadores, cartões magnéticos, “pen drives” ou qualquer outro meio de armazenamento, que por ventura tenha utilizado por ocasião da prestação de serviços.
- 24.15. Executar os serviços observando, rigorosamente, as especificações técnicas da CONTRATANTE, e em conformidade com as especificações estabelecidas na fase de nivelamento técnico.
- 24.16. Comunicar a CONTRATANTE, por escrito, qualquer anormalidade que possa colocar em risco o êxito e o cumprimento dos prazos, e metas propondo as ações e melhores soluções necessárias.
- 24.17. Obedecer, rigorosamente, as condições deste Termo de Referência, devendo qualquer alteração ser autorizada previamente por escrito pela CONTRATANTE.
- 24.18. Regularizar as possíveis irregularidades observadas no decorrer da entrega ou quando do funcionamento irregular, sem ônus e quando notificada pela CONTRATANTE, nas condições já previstos neste Termo de referência ,.
- 24.19. O fornecedor não poderá cobrar valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional.
- 24.20. Responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que os mesmos não têm nenhum vínculo empregatício com o Tribunal.
- 24.21. Fornecer todos os instrumentos necessários à execução dos serviços.
- 24.22. A contratada responderá integralmente por perdas e danos que vier a causar ao Tribunal ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

prepostos, independentemente de outras combinações contratuais ou legais a que estiver sujeita.

- 24.23. Responsabilizar-se técnica e administrativamente pelo objeto contratado, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.
- 24.24. Entregar os equipamentos em até 90 (noventa) dias após a assinatura do contrato, podendo ser prorrogado desde que precedido de justificativa acatada pelo CONTRATANTE.
- 24.25. Na hipótese de inexecução do objeto do Contrato, sem prejuízo da responsabilidade civil e criminal que couber, ficará a contratada sujeita às seguintes sanções: de multa diária, correspondente ao percentual de 0,17% sobre o respectivo valor do(s) item(ns) em atraso, até o limite máximo de 5%(cinco por cento) sobre o valor da parcela não executada, bem como sujeito a suspensão, pelo prazo de até 2 (dois) anos, de licitar e contratar com este Tribunal. O atraso superior a 30 dias poderá causar rescisão contratual.
- 24.26. Na hipótese de atraso injustificado da entrega dos equipamentos, fica estabelecido, a título de multa, por dia de atraso, até o limite máximo de 5%(cinco por cento).
- 24.27. Respeitar o prazo contratual de 12(doze) meses a partir de sua assinatura, prorrogáveis mediante formalização e assinatura das partes por igual período até o limite de 60(sessenta) meses.

**CRITÉRIOS E REQUISITOS DE HABILITAÇÃO 25.1.**

**QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

- 25.1.1. Certidão Negativa de Falência, Recuperação Judicial ou Extrajudicial expedida pelo distribuidor da sede do proponente, dentro do seu prazo de validade, e emitida no máximo com 120 (cento e vinte) dias de antecedência à data de abertura do pregão;
- 25.1.2. Balanço Patrimonial e Demonstrações Contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrado há mais de 03 (três) meses da data da apresentação da proposta;

Entende-se como “último exercício social já exigível” o Balanço Patrimonial e Demonstrações Contábeis encerrados em 31 de dezembro de 2020. Os prazos encerram-se em 31 de maio para as empresas que utilizam a ECD / SPED, e 30 de abril para as demais. Os balanços encerrados em 31 de dezembro de 2019 somente serão aceitos até as datas supracitadas.

As empresas obrigadas a usarem a Escrituração Contábil Digital – ECD, de acordo com a IN RFB 1.420/2013, deverão apresentar cópia do protocolo de transmissão ou recibo de entrega do SPED (Sistema Público de Escrituração

**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

Digital). As empresas que não são obrigadas a usarem a ECD / SPED, deverão apresentar o Balanço Patrimonial e Demonstrações Contábeis devidamente registrados na Junta Comercial.

No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

Não será exigido do licitante qualificado como microempresa ou empresa de pequeno porte a apresentação do Balanço Patrimonial e das Demonstrações Contábeis no caso de fornecimento de bens para pronta entrega, assim considerados aqueles que possuem entrega imediata, considerando o prazo de 30 (trinta) dias, de acordo com o art.6º, § único, da Lei Estadual nº 8.417, de 7 de novembro de 2016.

A comprovação da boa situação financeira da licitante será demonstrada através dos índices de Liquidez Geral - LG, Liquidez Corrente - LC e Solvência Geral - SG, que deverão ser maiores que um (>1), resultante da aplicação das fórmulas abaixo. Os índices deverão ser apresentados devidamente calculados e em ~~folha anexa ao Balanço Patrimonial.~~

$$\text{LG} = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Exigível a Longo Prazo}}$$
$$\text{LC} = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$
$$\text{SG} = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Exigível a Longo Prazo}}$$

O proponente deverá apresentar resultado maior que 1 (um) em todos os índices acima referidos, e deverá comprovar que possui capital mínimo ou patrimônio líquido no valor de 10% (dez por cento) da oferta apresentada, devendo a comprovação ser feita relativamente à data de sua apresentação, na forma da lei, admitida a atualização para esta data através de índices oficiais, para demonstrar sua boa situação financeira.

## **25.2. QUALIFICAÇÃO TÉCNICA**

25.2.1. As empresas deverão comprovar, como requisito de habilitação, registro ou inscrição regular no respectivo Conselho de Classe competente, de seu(s) responsável(is) técnico(s), da região a que estiverem vinculados, sendo inválida a certidão que não apresentar rigorosamente a situação atualizada.

25.2.2. As empresas deverão comprovar a qualificação técnica, como requisito de habilitação, comprovando também as seguintes exigências:

25.2.2.1. Comprovação de objeto social compatível com objeto desta licitação.

25.2.2.2. Aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, com o item pertinente mediante a

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
apresentação de ATESTADO(S) fornecido(s) por pessoas jurídicas de direito público ou privado, registrado no respectivo conselho de classe de registro da empresa e do profissional responsável.

25.2.2.3. Para fins da comprovação de que trata este subitem, os ATESTADOS deverão dizer respeito a serviços executados com as seguintes características mínimas:

- 25.2.2.3.1. Serviço de instalação de infraestrutura para rede de dados e voz, com cabeamento Estruturado UTP, tendo instalado no mínimo 200 (duzentos) pontos categoria 6 e 50 (cinquenta) pontos categoria 6A.
  - 25.2.2.3.2. Serviço de instalação de no mínimo 6 (Seis) racks;
  - 25.2.2.3.3. Execução de no mínimo 200 (duzentas) fusões de fibra óptica;
  - 25.2.2.3.4. Execução de no mínimo 100 (cem) certificações de fibra óptica;
  - 25.2.2.3.5. Serviço de instalação de no mínimo 2.000 (dois mil) metros de cabo de fibra óptica;
  - 25.2.2.3.6. Serviço de instalação e configuração de no mínimo 20 (vinte) câmeras IP;
  - 25.2.2.3.7. Serviço de instalação e configuração de software VMS;
  - 25.2.2.3.8. Serviço de instalação e configuração de no mínimo 2 (dois) switches de acesso e no mínimo 01 (um) switch core;
  - 25.2.2.3.9. Serviço de instalação e configuração de software de gerencia de rede;
  - 25.2.2.3.10. Serviço de instalação e configuração de no mínimo 15 (quinze) pontos de acesso sem fio.
  - 25.2.2.3.11. Serviço de instalação e configuração de software de controle de acesso de rede;
- 25.2.2.4. A escolha dos requisitos para comprovação da capacidade técnica operacional, deu-se pela seleção de itens que representam parcela relevante do objeto, conforme critérios técnicos e valores estimados foram selecionados os itens de maior relevância técnica do certame aqui trazidos.
- 25.2.2.5. O(s) atestado(s) apresentado(s) poderá(ão) ser objeto de diligência, a critério do pregoeiro, para a verificação da autenticidade do conteúdo das informações nele(s) contidas.
- 25.2.2.5.1. Nos casos em que houver necessidade de se realizar diligências posteriores, a critério do pregoeiro, o licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
local em que foram prestados os serviços.

- 25.2.2.5.2. O licitante será convocado a apresentar os documentos exigidos para a realização de diligências, em formato digital, via sistema, no prazo a ser estabelecido pelo pregoeiro, sob pena de inabilitação. O prazo estabelecido pelo pregoeiro não poderá ser inferior a 2 (duas) horas da convocação.
- 25.2.2.6. Não será permitida a soma de atestados para atendimento a um mesmo item.
- 25.2.2.7. A empresa CONTRATADA deverá encaminhar junto ao contrato assinado, comprovante mínimo de 02 profissionais da equipe técnica aptos a realizarem os trabalhos dentro das normas NR 10 e NR 35 ou apresentar os certificados de pelo menos dois membros da equipe técnica da empresa, caso na equipe haja profissional em engenharia elétrica apenas mais um profissional.
- 25.2.2.8. Todas as exigências técnicas de características contidas nos itens (equipamentos, acessórios, cabos, etc.) contidas neste Termo de Referência, deverão ser comprovadas, nos termos exigidos, mediante apresentação, por inclusão junto aos documentos de habilitação no cadastro da proposta eletrônica, antes disputa por lances, devendo serem apresentados todos os catálogos, datasheets e links oficiais do respectivo fabricante, necessários à comprovação das características técnicas, sob pena de inabilitação da proposta.
- 25.2.2.9. A comprovação de atendimento às exigências técnicas deste Termo de Referência são condições necessária para habilitação da proposta vencedora.

### **25.3. CONDIÇÕES PARA PAGAMENTO**

- 25.4. Nos preços constantes da proposta vencedora deverão estar inclusas todas as despesas, tais como: taxas, impostos, frete, seguro, embalagens, manuais e durante o período de garantia de funcionamento.
- 25.5. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.
- 25.6. Nos termos do artigo 36, §6º, da Instrução Normativa STI/MPOG nº 02, de 2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:
- 25.6.1. Não produziu os resultados acordados;
- 25.6.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

- 25.7. A Contratada regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário.
- 25.8. É condição para o pagamento do valor constante na Nota Fiscal/Fatura a apresentação, no momento da liquidação da empresa, de prova de regularidade no SICAF, ou mediante a expedição dos seguintes documentos:
- 25.8.1. Certidão Negativa (ou positiva com efeito de negativa) de Débito (CND), fornecida pelo Instituto Nacional de Seguro Social (INSS), disponibilizada em:
- a) <http://www.receita.fazenda.gov.br/previdencia/cnd/defaultpj.htm>.
- 25.8.2. Certidão de Regularidade do FGTS – CRT, emitido pela Caixa Econômica Federal, disponibilizada em:
- <https://www.sifge.caixa.gov.br/Cidadao/Crf/FgeCfSCriteriosPesquisa.asp>
- 25.8.3. Certidão Conjunta Negativa (ou Positiva com Efeito Negativa) de Débitos relativos aos TRIBUTOS FEDERAIS e à DIVIDA ATIVA DA UNIÃO, emitida pela Secretaria da Receita Federal, disponibilizada em:
- i) <http://www.receita.fazenda.gov.br/Certidoes/PessoaJuridica.htm>
- 25.8.4. Certidão Negativa de DÉBITOS TRABALHISTAS (ou Positiva com Efeito Negativa) perante a Justiça do Trabalho nos termos do Título VII-A da Consolidação das Leis do Trabalho, disponibilizada em:
- j) <http://www.tst.jus.br/certidao>.
- 25.8.5. Certidão Conjunta Negativa (ou Positiva com Efeito Negativa) de Débitos relativos aos TRIBUTOS ESTADUAIS e à DÍVIDA ATIVA DO ESTADO para as empresas inscritas no Estado do Pará; ou Certidão Negativa (ou Positiva com Efeito de Negativa) de DÉBITO DO ESTADO do domicílio ou sede da CONTRATADA.
- 25.8.6. Certidão Negativa de TRIBUTOS DO MUNICÍPIO, da sede da CONTRATADA.

## 26. REAJUSTE

- 26.1. Os preços são fixos e irrevogáveis no prazo de 12 (doze) meses contados da assinatura do contrato.
- 26.2. Dentro do prazo de vigência do contrato e mediante solicitação da CONTRATADA, os preços contratados poderão sofrer reajuste após o interregno de 12 (doze) meses contados da data de assinatura do contrato, aplicando-se o Índice de Preços ao Consumidor Amplo - IPCA, ou outro índice oficial que vier a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência do prazo

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
acima mencionado.

- 26.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
- 26.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE, pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.
- 26.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.
  - 26.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
- 26.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
- 26.8. O reajuste será realizado por apostilamento.
- 26.9. O reajuste somente será concedido após análise pelo setor competente e mediante motivação e comprovação, por parte da CONTRATADA.
- 26.10. A utilização do o Índice de Preços para o Consumidor Amplo - IPCA se justifica por se tratar de contratação de serviço de tecnologia da informação e ainda visando à recomposição dos valores contratados em vista dos efeitos inflacionários, além de ser mais vantajoso para a Administração.

## **27. REEQUILIBRIO ECONÔMICO-FINANCEIRO**

- 27.1. Com vistas a manutenção do equilíbrio econômico-financeiro do Contrato, poderá ser promovida revisão do preço contratual, desde que eventuais solicitações nesse sentido estejam acompanhadas de comprovação da superveniência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, configurando álea econômica extraordinária e extracontratual, bem como de demonstração analítica de seu impacto nos custos do Contrato, nos termos do disposto no art. 65, inciso II, alínea “d”, da lei nº 8.666/93.

## **28. GARANTIAS**

### **28.1. GARANTIA TÉCNICA**

- 28.1.1. A CONTRATADA deverá proceder com a confecção do plano de garantia e suporte técnico, indicando os canais de acionamento e abertura de chamados, com indicação dos horários de atendimento e canais de comunicação disposto neste Termo de Referência.

### **28.2. GARANTIA CONTRATUAL**

- 28.2.1. A CONTRATADA deverá apresentar a garantia de execução contratual de 5%

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
(cinco por cento), sobre o valor global da contratação, em uma das modalidades previstas no §1º do art. 56 da Lei Federal n.º 8.666/93, no momento da assinatura do contrato.

## **29. DISPOSIÇÕES GERAIS**

- 29.1. Em caso de divergência entre este Termo de Referência do Edital, prevalecerá este Termo de Referência.
- 29.2. A proposta deverá ser realizada contendo marca, modelo, fabricante e part number, desde o cadastramento na forma eletrônica para participação da disputa, de forma que a proposta não possibilite qualquer dubiedade de interpretação ou alteração do objeto ofertado, que em caso de descumprimento poderá sofrer pena de desclassificação.
- 29.3. Os equipamentos e serviços ofertados deverão atender aos itens discriminados nas especificações técnicas. O não atendimento de apenas um subitem será suficiente para a desclassificação da proposta.
- 29.4. Os equipamentos ofertados deverão ser novos, respeitando a especificações exigidas e as normas da ANATEL.
- 29.5. Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante). Deve ser comprovado por documento oficial do fabricante que não está em *end of sale*. Deve estar nas condições originais de fabricação, ou seja, sem modificação, retirada ou acréscimo de componentes externos e/ou internos à montagem original do fabricante ou acréscimo de componentes externos e/ou internos à montagem original do fabricante;
- 29.6. A licitante deverá apresentar documentação técnica oficial e original (ex: especificações, catálogos, prospectos e folders , links do fabricante) de todos os equipamentos ofertados que serão instalados no CONTRATANTE, no cadastramento da proposta sob pena de desclassificação.
- 29.7. Caso solicitado pela contratante, a indicação de determinada(s) característica(s) técnica(s) não encontrada(s) na documentação enviada, o licitante deverá emitir um documento no qual relacione, “ponto-a-ponto”, de cada sub-item de cada item, exigidos nas “Especificações Técnicas do Objeto”, e indicando, de maneira clara e direta, o documento apresentado e a página na qual se encontra a comprovação de que atende cada um dos subitens de cada item(ns) mencionado(s).
- 29.8. Os referidos documentos técnicos, contendo as especificações dos produtos ofertados em cumprimento as características exigidas, deverão estar atualizados em sua última versão de conteúdo, de publicação em site oficial, e de forma a não causar divergências de informações entre as diversas fontes oficiais disponibilizadas pelos fabricantes dos equipamentos, incluindo-se os “sites” oficiais dos fabricantes na internet.
- 29.9. Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado como características e funcionalidades técnicas e demais exigências de cada item constante no termo de referência em substituição ou complementação das exigidas documentação técnica oficial e original (catálogos, folders, *data sheets*, links

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO  
oficiais do site do fabricante etc.) exceto a questão de *end of sale* dos produtos.

- 29.10. O fornecedor deverá entregar, em 1 (uma) via, preferencialmente através de link de acesso oficial ou por documento digital, da documentação técnica constituída por manuais de instalação, configuração e operação, em português ou inglês, para cada um dos equipamentos e programas fornecidos.
- 29.11. Todos os programas fornecidos deverão ser entregues em mídia digital ou links de acesso do fabricante para cada um dos equipamentos onde serão instalados.
- 29.12. A Proponente deverá apresentar em sua proposta comercial o valor total objeto do presente registro de preços.
- 29.13. Constitui parte deste Termo de Referência o Termo de Confidencialidade. O termo de Confidencialidade estabelece de condições específicas para regulamentar as obrigações de sigilo a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações confidenciais e reservadas, disponibilizadas pela Contratante, por força dos procedimentos necessários para a execução do objeto do Contrato Principal a ser celebrado entre as partes, nos termos do modelo anexo.

Belém, 28 de setembro de 2021

**MARCUS ANTONIO DE SOUZA**

Diretor de Tecnologia da Informação