ESP-CORREGEDORIA DA POLICIA MILITAR

Termo de Referência 85/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
85/2026	180184-ESP-CORREGEDORIA DA POLICIA MILITAR	JULIANA NASCIMENTO FERREIRA DE JESUS	17/09/2026 08:25 (v 0.7)

Status
ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		057.00257770/2026-04

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de serviços de **solução integrada de Tecnologia da Informação e Comunicação (TIC)** nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste Termo de Referência, de acordo com as subdivisões na forma de itens que compõem este instrumento.

ITEM	*ESPECIFICAÇÃO*	*CATSER*	*UNIDADE DE MEDIDA*	*QUANTIDADE TOTAL*	*VALOR UNITÁRIO*	*VALOR TOTAL*
1	Contratação de serviços de expansão do armazenamento com fornecimento de servidores e renovação de licenças e garantias do Data Center	*27464*	*Unidade*	*01*	***R$5.895.300,00***	***R$5.895.300,00***

1.1.1. Em caso de eventual divergência entre a descrição do item do catálogo do sistema Compras.gov.br e as disposições deste Termo de Referência, prevalecem as disposições deste Termo de Referência.

1.1.2. Este Termo de Referência foi elaborado em conformidade com o **Decreto estadual nº 68.185, de 11 de dezembro de 2023**.

1.1.3. O objeto desta contratação não se enquadra como bem ou serviço de luxo, observando os limites estabelecidos no **Decreto estadual nº 67.985, de 27 de setembro de 2023**.

1.2. Os serviços objeto desta contratação são caracterizados como **serviço comum de Tecnologia da Informação e Comunicação (TIC)**, conforme justificativa constante do Estudo Técnico Preliminar, elaborado nos termos do Decreto estadual nº 68.017, de 11 de outubro de 2023.

1.3. O prazo de vigência da contratação é de 90 (noventa) dias, contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133, de 2021.

1.4. O contrato estabelece a disciplina que será aplicada em relação à vigência da contratação.

1.5. O Contratado não poderá subcontratar, ceder ou transferir, total ou parcialmente, o objeto contratual.

2. FUNDAMENTAÇÃO E DESCRIÇÃO CONTRATAÇÃO

2.1. A fundamentação da contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, nos termos do Decreto Estadual nº 67689, de 03 de maio de 2023, conforme detalhamento a seguir:

2.2.1. ID PCA no PNCP: 46377800000127-0-000166/2026;
2.2.2. Data de publicação no PNCP: 30/06/2025;
2.2.3. Id do item no PCA: 283;
2.2.4. Classe/Grupo: 166 - Serviços de Manutenção e Instalação de Equipamentos de TIC;

2.2.5. Identificador da Futura Contratação: 180184-20/2026.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Sustentabilidade

4.1.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos:

4.1.1.1. Comprovação de que os equipamentos fornecidos possuem certificações de baixo consumo energético (ex: *Energy Star* ou equivalente);

4.1.1.2. Adoção de arquitetura compatível com indicadores de eficiência energética (ex: métricas de *Power Usage Effectiveness* - PUE);

4.1.1.3. Apresentação de plano para o descarte e destinação ambientalmente adequada dos materiais e hardwares substituídos, observando a Política Nacional de Resíduos Sólidos.

4.2. Indicação de marcas ou modelos:

4.2.1. Na presente contratação será admitida a indicação da marca, **Dell, modelo PowerEdge R770**, de acordo com as justificativas contidas no Estudo Técnico Preliminar.

4.3. Da exigência de carta de solidariedade

4.3.1. Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

4.4. Garantia da contratação:

4.4.1. Não haverá exigência da garantia da contratação dos arts. 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

4.5. Vistoria

4.5.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 08 (oito) horas às 17 (dezessete) horas.

4.5.2. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.5.3. Para a vistoria, o representante legal do fornecedor ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pelo fornecedor comprovando sua habilitação para a realização da vistoria.

4.5.4. Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal de seu representante legal de que conhece o local e as condições da realização do objeto, ou declaração formal assinada por seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

4.5.5. O interessado não poderá pleitear modificações nos preços, nos prazos ou nas condições contratuais, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou de informações sobre o local em que será realizado o objeto da contratação.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. A execução do objeto seguirá a seguinte dinâmica:

5.1.1. Início da execução do objeto: em até 45 (quarenta e cinco) dias a contar da assinatura do contrato;

5.1.2. Descrição detalhada das rotinas e etapas, tecnologias, procedimentos, frequência e periodicidade de execução do trabalho:

Etapa	Atividades Focadas no Objeto	Período de Execução	Marco de Validação (Milestone)
1. Entrega & Recebimento Provisório	Entrega do hardware, conferência física de itens e entrega das chaves virtuais de licenciamento.	**Em até 45 (quarenta e cinco) dias a contar da assinatura do contrato**	**Termo de Recebimento Provisório (TRP)**
2. Montagem & Infraestrutura Física	Racking, cabeamento estruturado, conexões elétricas e atualização de firmware/BIOS dos servidores e switches.	**Em até 60 (sessenta) dias a contar da assinatura do contrato**	Relatório de Montagem Física Concluído
3. Ativação de Licenças & Virtualização	Implantação de hypervisors, ativação de licenças de S.O./Virtualização/Storage e vinculação nos portais dos fabricantes.	**Em até 60 (sessenta) dias a contar da assinatura do contrato**	Certificado de Ativação de Licenciamento
4. Configuração de Ambientes & Segurança	Provisionamento de storages, VLANs, regras de firewall, políticas de backup e integração com diretórios corporativos (AD /LDAP).	**Em até 60 (sessenta) dias a contar da assinatura do contrato**	Ambiente Base Pronto para Cargas
5. Testes de Homologação	Testes de carga, validação de Alta Disponibilidade (HA) e transferência de conhecimento/treinamento.	**Em até 75 (sessenta) dias a contar da assinatura do contrato**	Plano de Migração & Treinamento Concluídos
6. Encerramento & Aceite Definitivo	Validação final dos SLAs de execução, entrega da documentação *As-Built* e emissão do aceite final.	**Em até 75 (sessenta) dias a contar da assinatura do contrato**	**Termo de Recebimento Definitivo (TRD)**

5.2. Os serviços serão prestados na Rua Alfredo Maia, 58, Luz, São Paulo/SP;

5.3. Os serviços serão prestados de segunda a sexta-feira, no horário compreendido entre às 08h e 18h.

5.4. Rotinas a serem cumpridas:

5.4.1. Reunião de Alinhamento Inicial (*Kick-off Meeting*): Realizada no primeiro dia útil após a assinatura do contrato para alinhamento das equipes técnica e administrativa, definição de canais de comunicação, validação do cronograma detalhado e apresentação do Gestor e Fiscal do Contrato.

5.4.2. Recebimento e Inspeção Física (Recebimento Provisório): Conferência da entrega física dos equipamentos (*hardware*), verificação de integridade de embalagens, checagem de *part numbers*, números de série e entrega das chaves/chaves virtuais de licenciamento, culminando na emissão do **Termo de Recebimento Provisório (TRP)** em até 15 dias corridos.

5.4.3. Instalação, Configuração e Implantação: Execução dos serviços técnicos de montagem física em rack, conexão elétrica/lógica, atualização de *firmware*, ativação dos softwares/licenças e configuração do ambiente corporativo conforme especificações do Termo de Referência.

5.4.4. Migração, Testes e Homologação: Execução da migração de dados/sistemas, realização de testes de estresse, validação de mecanismos de Alta Disponibilidade (HA) e transferência de conhecimento/treinamento técnico para a equipe do contratante.

5.4.5. Fiscalização e Acompanhamento Contínuo: Registro diário de ocorrências em diário de obras /serviços pelo Fiscal do Contrato, aplicação do Instrumento de Medição de Resultado (IMR) e validação dos níveis de serviço (SLA) pactuados.

5.4.6. Vistoria Final e Aceite Definitivo (Recebimento Definitivo): Verificação integral do funcionamento da solução e entrega da documentação *As-Built*. Estando tudo em conformidade, será emitido o **Termo de Recebimento Definitivo (TRD)** até o limite fixado no cronograma (04/12).

5.4.7. Atesto e Liquidação Orçamentária: Apresentação da Nota Fiscal/Fatura pela contratada acompanhada do TRD, atesto formal pelo Fiscal/Gestor e encaminhamento ao setor financeiro para liquidação da despesa e pagamento dentro do exercício fiscal vigente (até 15/12).

5.4.8. Rotina de Chamados Técnicos: Prestação de atendimento técnico corretivo ou preventivo em resposta à abertura de chamado pela CONTRATANTE ou por detecção de necessidade no ambiente (ex.: liberação de pacotes de correção pelo fabricante), observando as seguintes condições:

5.4.8.1. A abertura de chamado técnico poderá ocorrer em qualquer dia da semana e em qualquer horário (regime 24/7);

5.4.8.2. O acionamento será realizado por meio de ligação telefônica, e-mail ou sistema informatizado oficial da CONTRATADA, devendo todos os canais garantir o registro auditável da demanda;

5.4.8.3. Cada chamado técnico deverá receber número de protocolo único e inequívoco para acompanhamento formal do processo;

5.4.8.4. Os atendimentos presenciais ou remotos deverão ser executados por técnico qualificado da CONTRATADA, acompanhados por representante da CONTRATANTE e previamente agendados;

5.4.8.5. A CONTRATADA deverá disponibilizar atendimento em língua portuguesa, sendo aceita a língua inglesa apenas para termos técnicos, manuais e documentação de software/hardware.

5.4.9. Relatório Mensal de Chamados: A CONTRATADA deverá apresentar periodicamente a relação analítica de todos os chamados técnicos do período, contendo:

5.4.9.1. Identificação do problema, nível de severidade e histórico com data/hora de início e término da solução (provisória e definitiva);

5.4.9.2. Detalhamento do diagnóstico e das providências adotadas;

5.4.9.3. Identificação do técnico da CONTRATADA responsável e do servidor do Departamento de Tecnologia da Informação (DTI) solicitante/validador.

5.4.10. Níveis de Serviço e Prazos de Solução:

5.4.10.1. Contato Inicial: Em até 2 (duas) horas da abertura, contatar a equipe da CONTRATANTE para alinhamento e posicionamento dos procedimentos a serem adotados;

5.4.10.2. Atendimento Crítico / Desempenho Degradado: Em até 6 (seis) horas da abertura, concluir o atendimento e restaurar o ambiente ao modo normal de operação;

5.4.10.3. Atendimento Não Crítico: Em até 24 (vinte e quatro) horas da abertura, concluir e finalizar o chamado técnico;

5.4.10.4. Limite de Indisponibilidade: Nas intervenções que exijam a interrupção (mesmo que parcial) dos serviços, o tempo total acumulado de indisponibilidade não poderá exceder a 4 (quatro) horas.

5.4.11. Regras para Substituição de Software e Licenciamento:

5.4.11.1. Na necessidade de substituição de software (fora dos casos de atualização de versão), a CONTRATADA deverá fornecer solução que atenda integralmente às funcionalidades da anterior;

5.4.11.2. Os softwares, licenças e insumos deverão ser fornecidos garantindo o pleno licenciamento e funcionamento do ambiente da CONTRATANTE;

5.4.11.3. A CONTRATADA deverá providenciar a renovação do suporte técnico oficial de todas as licenças do software de gerenciamento centralizado de virtualização (VMware) durante a vigência do contrato.

5.4.12. Regras para Substituição de Peças e Hardware:

5.4.12.1. Qualquer peça defeituosa deverá ser substituída por componente novo, original, sem uso anterior e tecnicamente compatível;

5.4.12.2. Se a troca do componente físico demandar adequações em nível de software, a execução e os custos serão de responsabilidade da CONTRATADA;

5.5. Materiais a serem disponibilizados

5.5.1. Para a perfeita execução dos serviços, o Contratado deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

5.5.1.1. Deverão ser fornecidos: 03 (três) servidores com as características abaixo:

5.5.1.2. Gabinete para instalação em rack de 19” através de sistema de trilhos deslizantes;

5.5.1.3. Altura mínima de 2U;

5.5.1.4. Deve possuir botão liga/desliga na parte frontal do equipamento;

5.5.1.5. Possuir display ou leds embutido no painel frontal do gabinete para exibição de alertas de funcionamento dos componentes internos, tais como falhas de memória RAM, fontes de alimentação, disco rígido e ventilador;

5.5.1.6. Possuir suporte de no mínimo 16 (dezesseis) baias para instalação de discos rígidos de 2.5 polegadas padrão SAS ou SATA;

5.5.1.7. Possuir suporte de no mínimo 8 (oito) baias para instalação de discos rígidos de 2.5 polegadas padrão NVMe;

5.5.1.8. Deverá ser entregue junto com o servidor, 01 (um) kit de fixação para rack, do tipo retrátil, permitindo o deslizamento do servidor e a organização dos cabos de alimentação e dados a fim de facilitar sua manutenção;

5.5.1.9. Deve possuir sistema de ventilação redundante e hot-pluggable para que a CPU suporte a configuração máxima e dentro dos limites de temperatura adequados para o perfeito funcionamento do equipamento, e que permita a substituição mesmo com o equipamento em funcionamento.

5.5.2. FONTE DE ALIMENTAÇÃO:

5.5.2.1 Mínimo de 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada;

5.5.2.2. Deverá ser fornecido com sua quantidade máxima de fontes;

5.5.2.3. As fontes deverão ser redundantes e hot-pluggable permitindo a substituição de qualquer uma das fontes em caso de falha sem parada ou comprometimento do funcionamento do equipamento; com potência mínima de 1500 watts;

5.5.2.4. As fontes devem possuir tensão de entrada de 100-240VAC a 60Hz;

5.5.2.5. Deverá acompanhar cabo de alimentação para cada fonte de alimentação fornecida.

5.5.3. PROCESSADOR:

5.5.3.1. Equipado com 02 (dois) processadores de 16 (dezesseis) núcleos, com arquitetura x86;

5.5.3.2. Deverá implementar mecanismos de gerenciamento do consumo de energia;

5.5.3.3. Deve suportar conjunto de instruções estendido compatível com padrão AVX-512;

5.5.3.4. Consumo de até 150W;

5.5.3.5. Tecnologia de no mínimo 10nm;

5.5.3.6. Frequência de clock interno de no mínimo 2.4 GHz;

5.5.3.7. Controladora de memória com suporte a DDR5 de no mínimo 6400 MHz;

5.5.3.8. Link de comunicação do processador com o restante do sistema de 24 GT/s;

5.5.3.9. Memória cache de 72 MB – L3.

5.5.4. MEMÓRIA RAM:

5.5.4.1. Módulos de memória RAM tipo DDR5 RDIMM (Registered DIMM) e velocidade de, no mínimo, 4800 MT/s;

5.5.4.2. Deve possuir no mínimo 32 slots de memória DIMM;

5.5.4.3. Suportar expansão de memória RAM para até no mínimo 8 TB (Oito Terabytes);

5.5.4.4. Deverá possuir 512 GB de memória distribuídos em módulos de no mínimo 64GB;

5.5.4.5. Só será aceita memórias do tipo RDIMM para a funcionalidade de memória RAM.

5.5.5. CIRCUITOS INTEGRADOS (CHIPSET) E PLACA MÃE:

5.5.5.1. O chipset deve ser da mesma marca do fabricante do processador;

5.5.5.2. Suportar, no mínimo, 4 (quatro) slots PCI Express 3.0, com a adição de módulos;

5.5.5.3. Placa mãe da mesma marca do fabricante do equipamento, devidamente compatível com o equipamento, desenvolvida especificamente para o modelo ofertado. Não serão aceitas placas de livre comercialização no mercado;

5.5.5.4. A Interface LOM deverá permitir substituição em campo, sem a necessidade de troca da placa mãe.

5.5.6. CONTROLADORA DE VÍDEO :

5.5.6.1. Deve ser do tipo on board (integrado na placa mãe);

5.5.6.2. Capacidade da memória cache de vídeo ou da placa de vídeo: mínimo de 16 MB (dezesseis megabytes);

5.5.6.3. Resolução gráfica de 1280 x 1024 pixels ou superior.

5.5.7. BIOS E SEGURANÇA:

5.5.7.1. BIOS desenvolvida pelo mesmo fabricante do equipamento, não sendo aceitas soluções em regime de OEM ou customizadas;

5.5.7.2. A BIOS deve possuir o número de série do equipamento e campo editável que permita inserir identificação customizada podendo ser consultada por software de gerenciamento, como número de propriedade e de serviço;

5.5.7.3. A BIOS deve possuir opção de criação de senha de acesso, senha de administrador ao sistema de configuração do equipamento;

5.5.7.4. Deve ser atualizável por software;

5.5.7.5. As atualizações de BIOS/UEFI devem possuir (assinatura) autenticação criptográfica segundo as especificações NIST SP800-147B e NIST SP800-155;

5.5.7.6. Deve possuir funcionalidade de recuperação de estado da BIOS/UEFI a uma versão anterior gravada em área de memória exclusiva e destinada a este fim, de modo a garantir recuperação em caso de eventuais falhas em atualizações ou incidentes de segurança;

5.5.7.7. Deverá ser fornecido com Módulo TPM 2.0;

5.5.7.8. Deverá ser fornecido tampa frontal;

5.5.7.9. Deverá emitir alerta de abertura do gabinete;

5.5.7.10. Por solicitação da licitante o equipamento poderá ser fornecido de fábrica com senha única, individual e exclusiva afixada em uma etiqueta de difícil remoção.

5.5.8. PORTAS DE COMUNICAÇÃO:

5.5.8.1. Todos os conectores das portas de entrada/saída devem ser identificados pelos nomes ou símbolos;

5.5.8.2. Deverá ser fornecido com 3 portas USB;

5.5.8.3. Possuir, no mínimo, 2 (duas) portas de vídeo padrão VGA (DB-15) ou Displayport, uma localizada na parte frontal do gabinete e outra na parte traseira do gabinete;

5.5.8.4. Possuir, capacidade para no mínimo, 01 (uma) porta serial (DB-9).

5.5.8.5. Possuir porta USB frontal dedicada para gerência.

5.5.9. INTERFACE DE REDE 25 GBPS:

5.5.9.1. Possuir 08 (oito) interfaces de rede 25Gb SFP28;

5.5.9.2. Suportar taxa de transferência 25 Gbps;

5.5.9.3. Suporte ao protocolo de virtualização VMQ 4.4.10.4;

5.5.9.4. Suporte ao protocolo VXLAN 4.4.10.5.

5.5.9.5. Possuir tecnologia de processamento TCP/IP offload LSO, RSS e TSS.

5.5.10. CONTROLADORA RAID

5.5.10.1. Controladora RAID, compatível com discos rígido padrão SAS 12Gb/s e SATA 6Gb/s;

5.5.10.2. Memória cache de no mínimo, 8GB (oito gigabytes) sendo que esta quantidade total de memória cache poderá ser atendida através de uma ou no máximo duas placas instaladas no servidor;

5.5.10.3. Suportar e implementar RAID 0, 1, 5, 6, 10, 50 e 60;

5.5.10.4. Suportar a criação de RAID por API;

5.5.10.5. Suportar expansão de capacidade de formatação on-line;

5.5.10.6. A controladora RAID deverá possuir quantidade de canais para atender a todos os discos do chassi ofertado;

5.5.10.7. Permita detecção e recuperação automática de falhas e reconstrução, também de forma automática, dos volumes de RAID sem impacto para as aplicações e sem necessidade de reiniciar o equipamento;

5.5.10.8. Deverá permitir a operação em modo RAID e pass-through em discos distintos, ou fornecer controladora RAID e controladora pass-through;

5.5.10.9. Suporte a recursos de hot swap para as unidades de disco rígido; **5.5.10.10.** Suportar implementação de disco Global Hot-spare;

5.5.10.11. Suportar migração de nível de RAID;

5.5.10.12. Suportar Self-Monitoring Analysis and Reporting Technology (SMART).

5.5.11 ARMAZENAMENTO:

5.5.11.1. Armazenamento bruto (raw) composto por, no mínimo, 2 (duas) unidades do dispositivo de armazenamento de dados do tipo SAS de, no mínimo, 1.2 TB cada;

5.5.11.2. Deve ser do tipo hot plug e hot swap, que permita sua substituição sem necessidade de desligar o equipamento, garantindo a continuidade das operações sem impacto para as aplicações.

5.5.12. DISPOSITIVO PARA INSTALAÇÃO DO SISTEMA OPERACIONAL:

5.5.12.1. Deve possuir dispositivos internos do tipo M.2, redundantes (espelhado), para inicialização de S.O com capacidade mínima de 480GB;

5.5.12.2. Deve ser fornecida uma controladora de RAID exclusiva e dedicada para estes discos suportando configuração mínima de RAID 1 (mirroring).;

5.5.12.3. Estes discos deverão ser dedicado para a instalação do sistema operacional, ou de virtualização e ou hiperconvergência;

5.5.12.4. Não será aceita soluções baseadas em cartão SD ou similar;

5.5.12.5. Caso a solução ofertada não possua estes dispositivos, devem ser fornecidos dois discos do tipo SSD de, no mínimo, 1.92TB ligados em RAID1 através da controladora de discos não comprometendo as baixas frontais. Estes discos deverão ser dedicados para a instalação do sistema operacional ou de virtualização.

5.5.13. SISTEMA OPERACIONAL:

5.5.13.1. Acompanhar mídia de inicialização e configuração do equipamento contendo todos os drivers de dispositivos de forma a permitir a fácil instalação do equipamento;

5.5.13.2. Deverá ser fornecido o licenciamento necessário para inclusão no cluster Vmware existente no ambiente de produção;

5.5.13.3. O licenciamento VMware deverá ser fornecido para todos os cores do servidor pelo período de garantia do mesmo;

5.5.13.4. Deverá ser fornecido o licenciamento Windows Server Standard, licenciando os cores do servidor, para no 7 de 48 mínimo 8 Maquinas Virtuais;

5.5.13.5. O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers dos dispositivos, BIOS e Firmwares para o equipamento ofertado;

5.5.13.6. Apresentar declaração do fabricante informando que todos os componentes do objeto são novos (sem uso, reforma ou recondicionamento) e que não estão fora de linha de fabricação;

5.5.13.7. O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2019. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link: http://www. windowsservercatalog.com;

5.5.13.8. O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 9 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link: https://hardware.redhat.com/hwcert/index.cgi;

5.5.13.9. O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESXi 8.0 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da VMware no link: http://www.vmware. com/resources/compatibility.

5.5.14. SOFTWARE:

5.5.14.1. Deverá vir acompanhado de todos os drivers de todos os dispositivos opcionais e que compõe o hardware.

5.5.15. CERTIFICADOS:

5.5.15.1. Deverá ser entregue no dia do pregão a certificação comprovando que o equipamento está em conformidade com a norma IEC 60950, Energy Star e Inmetro;

5.5.15.2. O equipamento ofertado deve estar de acordo com as diretivas ROHS.

5.5.16. GERENCIAMENTO E INVENTÁRIO:

5.5.16.1. O equipamento deve possuir solução de gerenciamento do próprio fabricante através de recursos de hardware e software com capacidade de prover as seguintes funcionalidades:

5.5.16.1.1. Possuir software de gerência, com capacidade de gerenciamento remoto de um único equipamento (1:1) e vários equipamentos (1:N);

5.5.16.1.2. O equipamento deve possuir interface de rede dedicada para gerenciamento que suporte nativamente a atribuição de endereçamento IP dinâmico;

5.5.16.1.3. Permitir o monitoramento remoto, de todo o hardware das condições de funcionamento dos equipamentos e seus componentes, tais como: processadores, memória RAM, controladora RAID, discos, fontes de alimentação, NICs e ventiladores;

5.5.16.1.4. Suportar os protocolos de criptografia SSL para acesso Web e SSH para acesso CLI;

5.5.16.1.5. Emitir alertas de anormalidade de hardware através do software de gerência e suportar o encaminhamento via e-mail e trap SNMP;

5.5.16.1.6. Suportar autenticação local e através de integração com MS Active Directory/LDAP;

5.5.16.1.7. Deverá suportar autenticação de 2 fatores;

5.5.16.1.8. Permitir o controle remoto da console do servidor do tipo virtual KVM out-of-band, ou seja, independente de sistema operacional ou software agente;

5.5.16.1.9. Permitir a captura de vídeo ou tela de situações de falhas críticas de sistemas operacionais e inicialização do sistema (boot), possibilitando uma depuração mais aprimorada;

5.5.16.1.10. As funcionalidades de gerenciamento e monitoramento de hardware devem ser providas por recursos do próprio equipamento e independente de agentes ou sistema operacional;

5.5.16.1.11. Caso a console virtual deverá ser acessível via interface HTML5 ou caso necessite de algum tipo de plugin licenciado, por exemplo JAVA deverá ser fornecido o licenciamento por pelo menos 3 anos;

5.5.16.1.12. Suportar os protocolos de gerenciamento, IPMI e SNMP v1, v2c, v3, WMI, SSH, WS MAN e REDFISH;

5.5.16.1.13. Permitir customizar alertas e automatizar a execução de tarefas baseadas em script;

5.5.16.1.14. Deverá possuir integração com VMware vCenter e Microsoft System Center;

5.5.16.1.15. Interface de gerencia baseado em HTML5;

5.5.16.1.16. Permitir configurar os seguintes parâmetros de hardware, (WWN, BIOS, RAID, NIC, MAC, Virtual Mac address, ISCSI Name, Vlan e perfil de QOS), através de templates pré-definidos;

5.5.16.1.17. Permitir a instalação, update e configuração remota de sistemas operacionais, drivers e firmwares, através de solução de deployment compatível com a solução ofertada;

5.5.16.1.18. Permitir a criação de perfis (baselines) de configuração para etectar desvios relacionados ao firmware dos componentes de hardware;

5.5.16.1.19. Possuir informações de garantia e apresentar via relatório e ou scorecard, listando o tipo de garantia e data limite, em caso de limite informar via e-mail de forma automatizada para que seja possível ação da contratante;

5.5.16.1.20. Permitir a detecção de pré-falhas dos componentes de hardware;

5.5.16.1.21. Realizar a abertura automática de chamados sem intervenção humana, diretamente ao fabricante dos equipamentos em caso de falha de componentes de hardware;

5.5.16.1.22. Permitir ligar, desligar e reiniciar os servidores remotamente e independente de sistema operacional;

5.5.16.1.23. Deve possuir recurso remoto que permita o completo desligamento e reinicialização (Hard-Reset) remoto do equipamento através da interface de gerência ou através de solução alternativa (Hardware/Software);

5.5.16.1.24. Permitir a emulação de mídias virtuais de inicialização (boot) através de CD/DVD remoto, compartilhamentos de rede NFS/CIFS e dispositivos de armazenamento USB remotos;

5.5.16.1.25. Permitir acesso do tipo Console Virtual, do mesmo fabricante dos servidores ofertados, que permita gerenciar, monitorar e configurar parâmetros físicos dos servidores de forma remota e centralizada;

5.5.16.1.26. O software de gerenciamento deve realizar descoberta automática dos servidores, permitindo inventariar os mesmos e seus componentes;

5.5.16.1.27. Suportar o monitoramento remoto (1:1 e 1:N) do consumo de energia elétrico e temperatura dos servidores, através de exibição gráfica, e permitir gerenciar parâmetros de consumo de CPU, memória, IO e Motherboard, com geração de alertas;

5.5.16.1.28. Possuir configuração de alerta de consumo de energia para grupos de dispositivos;

5.5.16.1.29. Possuir controles de energia baseados no tempo (diariamente, semanalmente e ou faixa de datas);

5.5.16.1.30. Permitir configurar dispositivos individuais, grupos físicos e grupos lógicos;

5.5.16.1.31. Permitir comparação de dispositivos relacionado ao seu consumo, criando reports com equipamentos ociosos em consumo e os de maior consumo;

5.5.16.1.32. A interface de gerencia do servidor deve permitir a criação de grupos de modo a permitir o gerenciamento de outros servidores a partir de um único IP sem a necessidade de softwares adicionais;

5.5.16.1.33. Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer disco dentro do servidor, suportando, no mínimo discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de memória não volátil (SSDs e NVMe);

5.5.16.1.34. Deve possibilitar o download automático de atualizações de firmwares, BIOS e drivers diretamente do site do fabricante ou repositório local. As atualizações de firmwares, BIOS e drivers devem ser possuir tecnologia de verificação de integridade do fabricante, de modo a garantir a autenticidade da mesma;

5.5.16.1.35. Deverá ser fornecido software que realize a descoberta de ativos no datacenter como servidores, switch, storage do mesmo fabricante e de outros fabricantes usando o protocolo SNMP, assim como o gerenciamento básico (ativo ou desligado) de dispositivos e inventário de hardware para até 1500 dispositivos.

5.5.16.1.36. A solução de gerenciamento de servidores deve permitir o gerenciamento através de aplicação de gerenciamento via dispositivos moveis (smartphones e tablets) compatível com sistemas IOS e ou Android.

5.5.16.1.37. APP deverá estar disponível para download na Google Play Store e Apple APP Store. Deverá possui relatórios de status de garantia via interface de gerência.

5.5.17. SWITCH CONFIGURAÇÃO FIXA 32 PORTAS 100 GBPS LAYER 3

5.5.17.1. Deverá ser fornecido 2 (dois) switches para produção com as características abaixo:

5.5.17.2. O switch Ethernet deve possuir pelo menos 32 (trinta e duas) portas 100 GB QSFP28 auto-sensing;

5.5.17.3. Possuir matriz de comutação de pelo menos 3.2 Tbps;

5.5.17.4. Possuir capacidade de processamento de pelo menos 2900Mpps (milhões de pacotes por segundo);

5.5.17.5. Possuir capacidade para no mínimo 90.000 endereços MAC;

5.5.17.6. Possuir LEDs, por porta, que indiquem a integridade e atividade do link;

5.5.17.7. Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação;

5.5.17.8. Todas as licenças necessárias para as funcionalidades exigidas neste edital deverão estar inclusas no equipamento;

5.5.17.9. Possuir fonte de alimentação interna redundante ao equipamento com ajuste automático de tensão;

5.5.17.10. Instalável em rack padrão de 19”, sendo que deverão ser fornecidos os respectivos kit’s de fixação;

5.5.17.11. O switch deve suportar Jumbo Frames de 9216 bytes;

5.5.17.12. Deverá acompanhar todos os cabos, transceivers e acessórios para conectividade do ambiente deste termo de referência.

5.5.18. FUNCIONALIDADES GERAIS:

5.5.18.1. Deve possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou RS-232 ou USB ou mini-USB;

5.5.18.2. Deve possuir uma interface de gerenciamento baseada em CLI (command line) completo com suporte a todos os comandos que permita aos usuários configurar e gerenciar switches através via Telnet e SSH;

5.5.18.3. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada;

5.5.18.4. Deve possuir espelhamento de porta remota;

5.5.18.5. Deve ser gerenciável via SNMP v3;

5.5.18.6. Deve possuir nativamente no mínimo 4 grupos RMON (History, Statistics, Alarms e Events);

5.5.18.7. Deve implementar Syslog em IPv4 para funções de “logging” de eventos;

5.5.18.8. Deve possuir o protocolo NTP ou SNTP para sincronismo de relógio do equipamento;

5.5.18.9. Deve implementar autenticação via RADIUS e TACACS;

5.5.18.10. Possuir suporte ao protocolo de autenticação para controle do acesso administrativo ao equipamento;

5.5.18.11. Deve implementar controle de acesso por porta de acordo com o padrão IEEE 802.1x;

5.5.18.12. Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino (IPv4 e IPv6), portas TCP e UDP de origem e destino e endereços MAC de origem e destino;

5.5.18.13. Possuir controle de broadcast e multicast;

5.5.18.14. Implementar sFlow ou similar;

5.5.18.15. Suporte a RDMA;

5.5.18.16. Suporte a RoCEv2;

5.5.18.17. Suporte a DCBX;

5.5.18.18. Implementar pelo menos 8 (oito) filas de saída por porta;

5.5.18.19. Implementar pelo menos uma fila de saída com prioridade estrita (ST) por porta e divisão ponderada (WRED, WRR ou similar) de banda entre as demais filas de saída;

5.5.18.20. Implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

5.5.18.21. Implementar classificação de tráfego baseada em endereço de origem/destino (IPv4 ou IPv6), portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

5.5.19. FUNCIONALIDADES DE CAMADA 2 (VLAN, SPANNING TREE):

5.5.19.1. Deve possuir LANs Virtuais (VLANs) conforme definições do padrão IEEE 802.1Q;

5.5.19.2. Deve permitir a criação de no mínimo 4000 VLANs;

5.5.19.3. Deve suportar VLANs dinâmicas permitindo a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;

5.5.19.4. Deve implementar “VLAN Trunking” conforme padrão IEEE 802.1Q. Deve ainda ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados;

5.5.19.5. Deve implementar LACP conforme padrão IEEE 802.3ad; 4.5.3.6.

5.5.19.6. Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d;

5.5.19.7. Deve implementar o padrão IEEE 802.1s (“Multiple Spanning Tree”), com suporte a no mínimo 15 instâncias simultâneas;

5.5.19.8. Deve implementar o padrão IEEE 802.1w (“Rapid Spanning Tree”);

5.5.19.9. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w);

5.5.19.10. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede.

5.5.20. FUNCIONALIDADES DE CAMADA 3 (MULTICAST E ROTEAMENTO):

5.5.20.1. Implementar IP multicast;

5.5.20.2. Implementar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse-mode”;

5.5.20.3. Implementar roteamento estático para no mínimo 16000 rotas IPv4;

5.5.20.4. Implementar roteamento dinâmico através dos protocolos RIPv1/RIPv2;

5.5.20.5. Implementar autenticação MD5 entre os peers RIPv2;

5.5.20.6. Implementar BGPv4;

5.5.20.7. Implementar protocolo de roteamento dinâmico OSPF v2 e v3;

5.5.20.8. Implementar o protocolo VRRP (Virtual Router Redundancy Protocol);

5.5.20.9. Implementar IGMPv1/V2/V3 Snooping.

5.5.21. SOLUÇÃO DE ARMAZENAMENTO PARA REPLICAÇÃO

5.5.21.1. A solução de armazenamento deverá integrar de maneira unificada ambientes “Block” (SAN) e “File” (NAS) através de um único equipamento não sendo aceitos equipamentos como gateways externos ou appliances;

5.5.21.2. Não serão admitidas soluções compostas pela união de dois ou mais subsistemas para a formação de cluster ou grid, devendo a oferta consistir num único equipamento com as características exigidas neste edital;Não serão admitidas soluções compostas pela união de dois ou mais subsistemas para a formação de cluster ou grid, devendo a oferta consistir num único equipamento com as características exigidas neste edital;

5.5.21.3. O hardware do subsistema de armazenamento e o software nele executado deverá ser do mesmo fabricante. O software de gerenciamento e monitoramento da solução deve ser nativo do próprio fabricante, sendo que não serão aceitas soluções baseadas em software Linux ou Windows;

5.5.21.4. Para o ambiente SAN deverá permitir os protocolos iSCSI e FC, de forma a ser possível a utilização dos protocolos ISCSI e FC simultaneamente;

5.5.21.5. Linux. Deverá possuir integração nativa com o Microsoft Windows Active Directory Service e LDAP em ambientes;

5.5.21.6. Para o ambiente NAS deverá permitir a utilização dos protocolos CIFS/SMB, NFS e FTP;

5.5.21.7. Deverá suportar o controle de quotas por pastas;

5.5.21.8. Deve possuir segurança de usuários de administração com nível de acesso diferenciado;

5.5.21.9. Deverá possuir login seguro com autenticação controlada pelo sistema de armazenamento ou integrada com Microsoft Active Directory (AD) com níveis de acesso diferenciado por grupos e pastas;

5.5.21.10. Permitir o agrupamento de múltiplas portas de redes, de modo a prover alta disponibilidade e balanceamento de carga distribuída de forma balanceada no sistema de armazenamento;

5.5.21.11. Deverá permitir o aumento imediato do tamanho dos volumes no sistema de armazenamento sem impacto para aos servidores ou clientes;

5.5.21.12. A solução Block e File deverá ser integrada a mesma ferramenta de gerência do sistema unificado com interface gráfica em Web;

5.5.21.13. A solução deverá ser nova, sem uso, e estar em linha de produção atual pelo fabricante no momento da entrega da proposta;

5.5.21.14. A solução deve ser compatível com gabinete padrão de mercado ou do fabricante e devem ser oferecidos todos os componentes, cabos, conectores, adaptadores, conversores, etc. necessários para a instalação, configuração e utilização da solução proposta;

5.5.21.15. A solução de armazenamento não deve apresentar ponto único de falha. Deve implementar failover automático e substituição de forma “Hot-Swappable” para os seguintes componentes: discos, controladoras, e fontes de alimentação. Deve suportar a manutenção ou substituição desses itens sem interrupção do funcionamento da solução;

5.5.21.16. A solução de armazenamento deverá suportar a aceleração de performance através da tecnologia SSD Cache para o nível de Bloco;

5.5.21.17. A solução de armazenamento deve permitir geração de snapshots (cópias de backup online ou point in time backup) a qualquer momento. A solução deve estar licenciada para realizar a capacidade máxima de snapshots suportada pelo equipamento. 5.2.21.18. A solução de armazenamento deve possuir funcionalidade de "thin provisioning", ou seja, a característica de consumir fisicamente apenas um percentual da capacidade máxima que o volume vai atingir no momento da criação;

5.5.21.18. A solução de armazenamento deve possuir funcionalidade de clonagem de áreas de dados contidos em volumes ou luns sem que se interrompa qualquer atividade de leitura ou escrita dos usuários ou aplicações aos dados;

5.5.21.19. A solução deverá estar licenciada para realizar a capacidade máxima de clones suportada pelo equipamento;

5.5.21.20. A solução de armazenamento deve contemplar a funcionalidade de recuperação de volume ou lun e arquivos, isto é, permitir ao administrador da solução restaurar esses objetos utilizando como base de recuperação os snapshots (cópias online no tempo) previamente gerados no storage;

5.5.21.21. A solução de armazenamento deve contemplar software para a replicação entre localidades remotas. A solução de replicação remota deve estar totalmente licenciada para a capacidade máxima suportada pelo 11 de 48 equipamento;

5.5.21.22. A replicação remota deverá permitir ser realizada de forma síncrona e assíncrona a nível de bloco;

5.5.21.23. A solução de armazenamento deve permitir a adição de capacidade ao volume, sem a descontinuidade do acesso à informação;

5.5.21.24. A solução de armazenamento deve possuir capacidade para a detecção de falhas, incluindo auto monitoração e geração de logs;

5.5.21.25. A solução de armazenamento deve ser compatível com sistemas operacionais Microsoft Windows, Vmware, Red Hat Enterprise Linux, SUSE Linux Enterprise, Sun Solaris;

5.5.21.26. A solução de storage deve possuir interface de gerenciamento gráfica GUI (Graphical User Interface) baseado em acesso Web e através de linha de comando CLI (Command Line Interface). Devendo possuir controle de acesso seguro por Telnet e SSH;

5.5.21.27. A solução deverá possuir capacidade para operar com discos nas tecnologias SSD, SAS e NL-SAS. O gabinete ou gaveta deverá dispor de slots “hot swappable” (substituíveis sem desligamento) para a acomodação dos discos;

5.5.21.28. A solução de armazenamento deve possuir software de gerenciamento com funções como: criação /administração de volumes, de thin provisioning, de raid group, de snapshots, de clones, de replicação, de thin clones e de usuários administradores;

5.5.21.29. A capacidade total de espaço de armazenamento da solução deve ser fornecida com as seguintes capacidades:

5.5.21.29.1. ÁREA 1: com no mínimo 53 TB brutos, com módulos de tecnologia SSD, cada módulo deverá possuir no máximo 7,68 TB.

5.5.21.29.2. ÁREA 2: com no mínimo 400 TB brutos, com módulos de tecnologia NL-SAS e discos com capacidade mínima de 24TB cada;

5.5.21.30. No caso de perda de qualquer disco do subsistema, independente da gaveta, slot ou localização física no array, deverá possuir e implementar a funcionalidade de “dynamic global sparing”, com alocação dinâmica e automática de um disco rígido físico como “hot spare”. Este disco deverá ser dedicado e exclusivo para esta função;

5.5.21.31. A solução de armazenamento deverá ter capacidade de crescimento para no mínimo 890 (oitocentos e noventa) módulos NVME através de escalabilidade vertical (com a adição de JBOD), através de conexões baseadas em tecnologia SAS de no mínimo 12Gb/s;

5.5.21.32. A solução de armazenamento deve possuir no mínimo:

5.5.21.32.1. 04 (quatro) interfaces de rede Ethernet de 25 Gb iSCSI (SFP28);

5.5.21.32.2. 02 (duas) interfaces de rede Ethernet de 100 Gb iSCSI (QSFP28);

5.5.21.33. A solução de armazenamento deverá permitir a expansão de interfaces com a adição de módulos:

5.5.21.33.1. 04 (quatro) interfaces Fibre Channel 32Gb/s;

5.5.21.34. O número máximo de cópias de snapshot por volume deverá ser e no mínimo 256 por volume e 4.096 para toda a solução de armazenamento de dados;

5.5.21.35. Os discos de reserva devem substituir qualquer disco defeituoso sem intervenção humana, de forma automática e sem parada do equipamento. Os discos de reserva devem ser de mesma tecnologia dos discos em produção;

5.5.21.36. A solução de armazenamento deve oferecer no mínimo os seguintes níveis de proteção RAID: 0, 1, 5, 6;

5.5.21.37. A solução de storage deve possuir, no mínimo, 192 (cento e noventa e dois) GB de memória cache ECC, somando-se a memória cache de todas as controladoras RAID;

5.5.21.38. A solução de storage deverá permitir a expansão futura com a adição de memória cache ECC, possibilitando a capacidade máxima de 384 (trezentos e oitenta e quatro) GB para a solução;

5.5.21.39. As controladoras devem possuir entre si mecanismo de espelhamento e proteção de cache de escrita de forma a garantir que a integridade e continuidade de funcionamento do storage mesmo com a falha de uma das controladoras;

5.5.21.40. A solução deve incluir suporte a multipathing (múltiplos caminhos) para acesso dos servidores aos discos virtuais criados no storage. O objetivo é oferecer caminhos redundantes entre storages e servidor;

5.5.21.41. A solução de armazenamento deve possuir uma ferramenta nativa do próprio sistema operacional para permitir a integração e gerenciamento dos dados para plataformas de nuvem (cloud)

públicas. A ferramenta deve ser capaz de prover funcionalidades conhecidas como Cloud Tiering, Cloud Cache e Cloud Replication para no mínimo as seguintes plataformas: Microsot Azure, Amazon S3 e Google Cloud;

5.5.21.42. Caso a solução ofertada não suporta a integração nativa com cloud exigida no item anterior, deverá ser fornecida uma volumetria adicional de 100% da capacidade de armazenamento.

5.5.22. APPLIANCE DE MONITORAMENTO:

5.5.22.1. Deverá ser entregue um appliance de gerenciamento remoto com as seguintes características:

5.5.22.1.1. O serviço fornecido deve utilizar dispositivo de hardware dedicado a função de monitoramento de infraestrutura, não sendo aceito soluções montadas sob a plataforma PC/x86 nem dispositivos montados usando soluções Open Source;

5.5.22.1.2. Deve permitir instalação em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;

5.5.22.1.3. Deve possuir, no máximo, 2 RU (Rack Unit) de altura;

5.5.22.1.4. Deve possuir 2 fontes de alimentação AC bivolt interna, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz);

5.5.22.1.5. Processador interno com quatro cores, Intel x86 ou equivalente, para permitir execução de aplicações internas tipo Dockers ou Kubernetes;

5.5.22.1.6. Deve possuir 16 (dezesseis) portas seriais com suporte a expansão até 80 (oitenta) portas seriais com conectores seriais RJ-45 em uma unidade “RU”, sem a utilização de switches externos;

5.5.22.1.7. Deve possuir 16 (dezesseis) portas Ethernet RJ-45 1 GbE, com suporte a expansão para até 48 (quarenta e oito) portas Ethernet;

5.5.22.1.8. Deve possuir para up-link ou aceso, no mínimo, 02 (duas) portas Gigabit Ethernet (10/100 /1000BT), com interface RJ-45 e 02 (duas) portas SFP+ 10GB;

5.5.22.1.9. Deve permitir o acesso opcional via rede móvel LTE 4G, devendo ser fornecido com chip de dados ativo;

5.5.22.1.10. Deve permitir o acesso opcional via rede Wifi através de módulos;

5.5.22.1.11. Permitir acesso pelos protocolos HTTPS, SSHv2; opcional HTTP, Telnet and SSHv1;

5.5.22.1.12. Permitir a configuração via interface Gráfica ou linha de comando e Linux;

5.5.22.1.13. Deve suportar no mínimo 32GB de armazenamento interno;

5.5.22.1.14. Deve suportar as funções de servidor DHCP e executar roteamento e funções de firewall;

5.5.22.1.15. Deve suportar plataforma para Automação para end device via, Puppet, Chef e Ansible;

5.5.22.1.16. Deve suportar automação via diferentes meios, incluindo, shell Scriipt, Cloud, RESTFUL, ANSIBLE, Chef, Docker, Puppet, Python, Ansible;

5.5.22.1.17. Permitir Agrupamento de equipamentos via software em grupos associando múltiplas unidades e permitir o gerenciamento através do login em uma das unidades apenas;

5.5.22.1.18. Console. Envio de alertas e eventos deve permitir envio de mensagens via log de sistema, E-mail e na própria console, suportar a customização do nível de acesso de usuários;

5.5.22.1.19. Deve suportar a descoberta automática de novos dispositivos;

5.5.22.1.20. Deve permitir configurar suporte a NTP, zonas de horários mundiais ou sincronização através de torre de celular;

5.5.22.1.21. Deve permitir a restrição do acesso à interface de linha de comando (CLI) através de senha e dupla autenticação usando protocolos RSA e DUO;

5.5.22.1.22. Deve suportar tunelamento através de SSL VPN, IPSec e Wireguard VPN;

5.5.22.1.23. Deve suportar mecanismos de AAA (Authentication, Authorization e Accounting), com suporte aos protocolos RADIUS e TACACS+, LDAP e Kerberos;

5.5.22.1.24. Deve suportar o protoco IPv6;

5.5.22.1.25. Deve permitir a configuração de endereços IPv6 para gerenciamento;

5.5.22.1.26. Deve suportar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH e HTTP sobre IPv6;

5.5.22.1.27. Deve suportar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6\ Suportar IPv4 / IPv6.

5.5.23. EXPANSÃO DO ARMAZENAMENTO:

5.5.23.1. A solução deverá expandir a atual solução de armazenamento em produção no ambiente da Corregedoria da Policia Militar do fabricante Dell EMC em 180 TB, conforme características abaixo:

5.5.23.1.1. A solução de armazenamento local deve ser compatível com a solução existente e devem ser oferecidos todos os componentes, cabos, conectores, adaptadores, conversores necessários para a instalação, configuração e utilização da solução proposta;

5.5.23.1.2. A solução de armazenamento local não deve apresentar ponto único de falha;

5.5.23.1.3. Deve implementar substituição de forma “Hot-Swappable” para os seguintes componentes: discos, 13 (treze) de 48 (quarenta e oito) controladoras e fontes de alimentação;

5.5.23.1.4. Deve suportar a manutenção ou substituição desses itens sem interrupção do funcionamento da solução;

5.5.23.1.5. Para fins de capacidade líquida de armazenamento de dados considerar que a área disponível para uso pelos usuários e aplicações deve excluir discos de paridade, discos de reserva, formatação dos discos e outras áreas nos discos necessárias para o funcionamento da solução;

5.5.23.1.6. A solução de armazenamento local deve suportar interfaces back end 12 Gb/s SAS;

5.5.23.1.7. A solução de armazenamento local Tier 2 deve ser fornecida baseado em discos NL-SAS;

5.5.23.1.8. O gabinete ou gaveta de discos deverá dispor de slots “hot swappable” (substituíveis sem desligamento) para a acomodação dos discos;

5.5.23.1.9. Os discos de reserva devem substituir qualquer disco defeituoso sem intervenção humana, de forma automática e sem parada do equipamento;

5.5.23.1.10. Os discos de reserva devem ser de mesma tecnologia dos discos em produção e deve vir configurado com pelo menos 01 (um) disco por gaveta;

5.5.23.1.11. A solução de armazenamento deverá ser fornecida com a capacidade bruta e configurada considerando-se os seguintes níveis: Nível (Tier) 2, de 180 TB Bruto em discos NL-SAS, 7.2K 12 Gbps, distribuídos em discos com no máximo 12 TB cada;

5.5.23.1.12. Deverá ser fornecida a renovação de toda solução pertinente a este item, controladoras principais e expansões para o período do presente certame.

5.5.24. SOLUÇÃO DE ARMAZENAMENTO EM DISCO:

5.5.24.1. A solução de armazenamento deverá integrar de maneira unificada ambientes “Block” (SAN) e “File” (NAS) através de um único equipamento não sendo aceitos equipamentos como gateways externos ou appliances;

5.5.24.2. Não serão admitidas soluções compostas pela união de dois ou mais subsistemas para a formação de cluster ou grid, devendo a oferta consistir num único equipamento com as características exigidas neste edital;Não serão admitidas soluções compostas pela união de dois ou mais subsistemas para a formação de cluster ou grid, devendo a oferta consistir num único equipamento com as características exigidas neste edital;

5.5.24.3. O hardware do subsistema de armazenamento e o software nele executado deverá ser do mesmo fabricante. O software de gerenciamento e monitoramento da solução deve ser nativo do próprio fabricante, sendo que não serão aceitas soluções baseadas em software Linux ou Windows;

5.5.24.4. Para o ambiente SAN deverá permitir os protocolos iSCSI e FC, de forma a ser possível a utilização dos protocolos ISCSI e FC simultaneamente;

5.5.24.5. Linux. Deverá possuir integração nativa com o Microsoft Windows Active Directory Service e LDAP em ambientes;

5.5.24.6. Para o ambiente NAS deverá permitir a utilização dos protocolos CIFS/SMB, NFS e FTP;

5.5.24.7. Deverá suportar o controle de quotas por pastas;

5.5.24.8. Deve possuir segurança de usuários de administração com nível de acesso diferenciado;

5.5.24.9. Deverá possuir login seguro com autenticação controlada pelo sistema de armazenamento ou integrada com Microsoft Active Directory (AD) com níveis de acesso diferenciado por grupos e pastas;

5.5.24.10. Permitir o agrupamento de múltiplas portas de redes, de modo a prover alta disponibilidade e balanceamento de carga distribuída de forma balanceada no sistema de armazenamento;

5.5.24.11. Deverá permitir o aumento imediato do tamanho dos volumes no sistema de armazenamento sem impacto para aos servidores ou clientes.

5.5.24.12. A solução Block e File deverá ser integrada a mesma ferramenta de gerência do sistema unificado com interface gráfica em Web;

5.5.24.13. A solução deverá ser nova, sem uso, e estar em linha de produção atual pelo fabricante no momento da entrega da proposta;

5.5.24.14. A solução deve ser compatível com gabinete padrão de mercado ou do fabricante e devem ser oferecidos todos os componentes, cabos, conectores, adaptadores, conversores, etc, necessários para a instalação, configuração e utilização da solução proposta;

5.5.24.15. A solução de armazenamento não deve apresentar ponto único de falha. Deve implementar failover automático e substituição de forma “Hot-Swappable” para os seguintes componentes: discos, controladoras, e fontes de alimentação. Deve suportar a manutenção ou substituição desses itens sem interrupção do funcionamento da solução;

5.5.24.16. A solução de armazenamento deverá suportar a aceleração de performance através da tecnologia SSD Cache para o nível de Bloco;

5.5.24.17. A solução de armazenamento deve permitir geração de snapshots (cópias de backup online ou point in time backup), a qualquer momento. A solução deve estar licenciada para realizar a capacidade máxima de snapshots suportada pelo equipamento;

5.5.24.18. A solução de armazenamento deve possuir funcionalidade de "thin provisioning", ou seja, a característica de consumir fisicamente apenas um percentual da capacidade máxima que o volume vai atingir no momento da criação;

5.5.24.19. A solução de armazenamento deve possuir funcionalidade de clonagem de áreas de dados contidos em volumes ou luns sem que se interrompa qualquer atividade de leitura ou escrita dos usuários ou aplicações aos dados. A solução deverá estar licenciada para realizar a capacidade máxima de clones suportada pelo equipamento;

5.5.24.20. A solução de armazenamento deve contemplar a funcionalidade de recuperação de volume ou lun e arquivos, isto é, permitir ao administrador da solução restaurar esses objetos utilizando como base de recuperação os snapshots (cópias online no tempo), previamente gerados no storage;

5.5.24.21. A solução de armazenamento deve contemplar software para a replicação entre localidades remotas. A solução de replicação remota deve estar totalmente licenciada para a capacidade máxima suportada pelo equipamento;

5.5.24.22. A replicação remota deverá permitir ser realizada de forma síncrona e assíncrona a um nível de bloco;

5.5.24.23. A solução de armazenamento deve permitir a adição de capacidade ao volume, sem a descontinuidade do acesso à informação;

5.5.24.24. A solução de armazenamento deve possuir capacidade para a detecção de falhas, incluindo auto monitoração e geração de logs;

5.5.24.25. A solução de armazenamento deve ser compatível com sistemas operacionais Microsoft Windows, Vmware, Red Hat Enterprise Linux, SUSE Linux Enterprise, Sun Solaris;

5.5.24.26. A solução de storage deve possuir interface de gerenciamento gráfica GUI (Graphical User Interface), baseado em acesso Web e através de linha de comando CLI (Command Line Interface). Devendo possuir controle de acesso seguro por Telnet e SSH;

5.5.24.27. A solução deverá possuir capacidade para operar com discos nas tecnologias SSD, SAS e NL-SAS. O gabinete ou gaveta deverá dispor de slots “hot swappable” (substituíveis sem desligamento), para a acomodação dos discos;

5.5.24.28. A solução de armazenamento deve possuir software de gerenciamento com funções como: criação /administração de volumes, de thin provisioning, de raid group, de snapshots, de clones, de replicação, de thin clones e de usuários administradores;

5.5.24.29. A capacidade total de espaço de armazenamento da solução deve ser fornecida com as seguintes capacidades:

5.5.24.29.1. ÁREA 1 com no mínimo 53 (cinquenta e três) TB brutos, com módulos de tecnologia SSD e capacidade mínima de 7,68TB;

5.5.24.29.2. ÁREA 2 com no mínimo 408 (quatrocentos e oito) TB brutos, com módulos de tecnologia NL-SAS e discos com capacidade mínima de 24 (vinte e quatro) TB cada;

5.5.24.30. No caso de perda de qualquer disco do subsistema, independente da gaveta, slot ou localização física no array, deverá possuir e implementar a funcionalidade de “dynamic global sparing”, com alocação dinâmica e automática de um disco rígido físico como “hot spare”. Este disco deverá ser dedicado e exclusivo para esta função;

5.5.24.31. A solução de armazenamento deverá ter capacidade de crescimento para no mínimo 890 (oitocentos e noventa) módulos NVME através de escalabilidade vertical (com a adição de JBOD), através de conexões baseadas em tecnologia SAS de no mínimo 12Gb/s.

5.5.24.32. A solução de armazenamento deve possuir no mínimo: 04 (quatro) interfaces de rede Ethernet de 25 Gb iSCSI (SFP28), sendo 02 (duas) interfaces de rede Ethernet de 100 Gb iSCSI (QSFP28);

5.5.24.33. A solução de armazenamento deverá permitir a expansão de interfaces com a adição de módulos com 04 (quatro) interfaces Fibre Channel 32Gb/s;

5.5.24.34. O número máximo de cópias de snapshot por volume deverá ser de no mínimo 256 (duzentos e cinquenta e seis) por volume, e 4.096 (quatro mil e noventa e seis) para toda a solução de armazenamento de dados;

5.5.24.35. Os discos de reserva devem substituir qualquer disco defeituoso sem intervenção humana, de forma automática e sem parada do equipamento. Os discos de reserva devem ser de mesma tecnologia dos discos em produção;

5.5.24.36. A solução de armazenamento deve oferecer no mínimo os seguintes níveis de proteção RAID: 0, 1, 5, 6;

5.5.24.37. A solução de storage deve possuir, no mínimo, 192 (cento e noventa e dois) GB de memória cache ECC, somando-se a memória cache de todas as controladoras RAID;

5.5.24.38. A solução de storage deverá permitir a expansão futura com a adição de memória cache ECC, possibilitando a capacidade máxima de 384 (trezentos e oitenta e quatro) GB para a solução;

5.5.24.39. As controladoras devem possuir entre si mecanismo de espelhamento e proteção de cache de escrita de forma a garantir que a integridade e continuidade de funcionamento do storage mesmo com a falha de uma das controladoras;

5.5.24.40. A solução deve incluir suporte a multipathing (múltiplos caminhos) para acesso dos servidores aos discos virtuais criados no storage. O objetivo é oferecer caminhos redundantes entre storages e servidor;

5.5.24.41. Deverá possuir o suporte para armazenamento de objetos via API Restful, permitindo a criação de buckets, gerenciamento de usuários, políticas de retenção diretamente no sistema de armazenamento;

5.5.24.42. A solução de armazenamento deve possuir uma ferramenta nativa do próprio sistema operacional para permitir a integração e gerenciamento dos dados para plataformas de nuvem (cloud) públicas. A ferramenta deve ser capaz de prover funcionalidades conhecidas como Cloud Tiering, Cloud Cache e Cloud Replication para no mínimo as seguintes plataformas: Microsot Azure, Amazon S3 e Google Cloud;

5.5.24.43. Caso a solução ofertada não suporta a integração nativa com cloud exigida no item anterior, deverá ser fornecida uma volumetria adicional de 100% da capacidade de armazenamento.

5.5.25. EXPANSÃO BIBLIOTECA DE FITAS:

5.5.25.1. Deverá ser fornecido uma expansão para o armazenamento de biblioteca de fitas ou a entrega de uma solução de armazenamento em disco conforme as características abaixo:

5.5.25.1.1. Expansão para a atual solução de biblioteca de fitas em produção no ambiente da Corregedoria da Policia Militar que utiliza atualmente do fabricante Dell EMC em 80 slots adicionais;

5.5.25.1.2. A expansão deve ser compatível com a solução existente e devem ser oferecidos todos os componentes, cabos, conectores, adaptadores, conversores necessários para a instalação, configuração e utilização da solução proposta;

5.5.25.1.3. Deverá ser fornecido 04 (quatro) drives LTO-9 Fibre Channel;

5.5.25.1.4. Deverá ser fornecida 160 (cento e sessenta) mídias LTO-9;

5.5.25.1.5. Deverá ser fornecida 02 (duas) placas Fibre Channel Dual Channel 8/16Gbps compatível com o servidor atual de backup.

5.5.26. CARACTERÍSTICAS PARA A SOLUÇÃO DE ARMAZENAMENTO:

5.5.26.1. A solução de armazenamento deverá integrar de maneira unificada ambientes “Block” (SAN) e “File” (NAS) através de um único equipamento não sendo aceitos equipamentos como gateways externos ou appliances;

5.5.26.2. Não serão admitidas soluções compostas pela união de dois ou mais subsistemas para a formação de cluster ou grid, devendo a oferta consistir num único equipamento com as características exigidas neste edital;Não serão admitidas soluções compostas pela união de dois ou mais subsistemas para a formação de cluster ou grid, devendo a oferta consistir num único equipamento com as características exigidas neste edital;

5.5.26.3. O hardware do subsistema de armazenamento e o software nele executado deverá ser do mesmo fabricante. O software de gerenciamento e monitoramento da solução deve ser nativo do próprio fabricante, sendo que não serão aceitas soluções baseadas em software Linux ou Windows;

5.5.26.4. Para o ambiente SAN deverá permitir os protocolos iSCSI e FC, de forma a ser possível a utilização dos protocolos ISCSI e FC simultaneamente;

5.5.26.5. Deverá possuir integração nativa com o Microsoft Windows Active Directory Service e LDAP em ambientes Linux;

5.5.26.6. Para o ambiente NAS deverá permitir a utilização dos protocolos CIFS/SMB, NFS e FTP;

5.5.26.7. Deverá suportar o controle de quotas por pastas;

5.5.26.8. Deve possuir segurança de usuários de administração com nível de acesso diferenciado;

5.5.26.9. Deverá possuir login seguro com autenticação controlada pelo sistema de armazenamento ou integrada com Microsoft Active Directory (AD) com níveis de acesso diferenciado por grupos e pastas;

5.5.26.10. Permitir o agrupamento de múltiplas portas de redes, de modo a prover alta disponibilidade e balanceamento de carga distribuída de forma balanceada no sistema de armazenamento;

5.5.26.11. Deverá permitir o aumento imediato do tamanho dos volumes no sistema de armazenamento sem impacto para aos servidores ou clientes;

5.5.26.12. A solução Block e File deverá ser integrada a mesma ferramenta de gerência do sistema unificado com interface gráfica em Web;

5.5.26.13. A solução deverá ser nova, sem uso, e estar em linha de produção atual pelo fabricante no momento da entrega da proposta;

5.5.26.14. A solução deve ser compatível com gabinete padrão de mercado ou do fabricante e devem ser oferecidos todos os componentes, cabos, conectores, adaptadores, conversores, etc. necessários para a instalação, configuração e utilização da solução proposta;

5.5.26.15. A solução de armazenamento não deve apresentar ponto único de falha. Deve implementar failover automático e substituição de forma “Hot-Swappable” para os seguintes componentes: discos, controladoras, e fontes de alimentação. Deve suportar a manutenção ou substituição desses itens sem interrupção do funcionamento da solução;

5.5.26.16. A solução de armazenamento deverá suportar a aceleração de performance através da tecnologia SSD Cache para o nível de Bloco;

5.5.26.17. A solução de armazenamento deve permitir geração de snapshots (cópias de backup online ou point in time backup), a qualquer momento. A solução deve estar licenciada para realizar a capacidade máxima de snapshots suportada pelo equipamento;

5.5.26.18. A solução de armazenamento deve possuir funcionalidade de "thin provisioning", ou seja, a característica de consumir fisicamente apenas um percentual da capacidade máxima que o volume vai atingir no momento da criação;

5.5.26.19. A solução de armazenamento deve possuir funcionalidade de clonagem de áreas de dados contidos em volumes ou luns sem que se interrompa qualquer atividade de leitura ou escrita dos usuários ou aplicações aos dados. A solução deverá estar licenciada para realizar a capacidade máxima de clones suportada pelo equipamento;

5.5.26.20. A solução de armazenamento deve contemplar a funcionalidade de recuperação de volume ou lun e arquivos, isto é, permitir ao administrador da solução restaurar esses objetos utilizando como base de recuperação os snapshots (cópias online no tempo) previamente gerados no storage;

5.5.26.21. A solução de armazenamento deve contemplar software para a replicação entre localidades remotas. A solução de replicação remota deve estar totalmente licenciada para a capacidade máxima suportada pelo equipamento;

5.5.26.22. A replicação remota deverá permitir ser realizada de forma síncrona e assíncrona a um nível de bloco;

5.5.26.23. A solução de armazenamento deve permitir a adição de capacidade ao volume, sem a descontinuidade do acesso à informação;

5.5.26.24. A solução de armazenamento deve possuir capacidade para a detecção de falhas, incluindo auto monitoração e geração de logs;

5.5.26.25. A solução de armazenamento deve ser compatível com sistemas operacionais Microsoft Windows, Vmware, Red Hat Enterprise Linux, SUSE Linux Enterprise, Sun Solaris;

5.5.26.26. A solução de storage deve possuir interface de gerenciamento gráfica GUI (Graphical User Interface) baseado em acesso Web e através de linha de comando CLI (Command Line Interface). Devendo possuir controle de acesso seguro por Telnet e SSH;

5.5.26.27. A solução deverá possuir capacidade para operar com discos nas tecnologias SSD, SAS e NL-SAS. O gabinete ou gaveta deverá dispor de slots “hot swappable” (substituíveis sem desligamento), para a acomodação dos discos;

5.5.26.28. A solução de armazenamento deve possuir software de gerenciamento com funções como: criação /administração de volumes, de thin provisioning, de raid group, de snapshots, de clones, de replicação, de thin clones e de usuários administradores;

5.5.26.29. A capacidade total de espaço de armazenamento da solução deve ser fornecida da seguinte forma: ÁREA 1 com no mínimo 860 TB brutos, com módulos de tecnologia NL-SAS e discos com capacidade mínima de 24TB cada;

5.5.26.30. No caso de perda de qualquer disco do subsistema, independente da gaveta, slot ou localização física no array, deverá possuir e implementar a funcionalidade de “dynamic global sparing”, com alocação dinâmica e automática de um disco rígido físico como “hot spare”. Este disco deverá ser dedicado e exclusivo para esta função;

5.5.26.31. A solução de armazenamento deverá ter capacidade de crescimento para no mínimo 890 (oitocentos e noventa) módulos NVME através de escalabilidade vertical (com a adição de JBOD), através de conexões baseadas em tecnologia SAS de no mínimo 12Gb/s;

5.5.26.32. A solução de armazenamento deve possuir no mínimo 04 (quatro) interfaces de rede Ethernet de 25 Gb iSCSI (SFP28), e 02 (duas) interfaces de rede Ethernet de 100 Gb iSCSI (QSFP28);

5.5.26.33. A solução de armazenamento deverá permitir a expansão de interfaces com a adição de módulos com 04 (quatro) interfaces Fibre Channel de 32Gb/s;

5.5.26.34. O número máximo de cópias de snapshot por volume deverá ser de no mínimo 256 (duzentos e cinquenta e seis), por volume, e 4.096 (quatro mil e noventa e seis), para toda a solução de armazenamento de dados;

5.5.26.35. Os discos de reserva devem substituir qualquer disco defeituoso sem intervenção humana, de forma automática e sem parada do equipamento. Os discos de reserva devem ser de mesma tecnologia dos discos em produção;

5.5.26.36. A solução de armazenamento deve oferecer no mínimo os seguintes níveis de proteção RAID: 0, 1, 5, 6, 10 e 50;

5.5.26.37. A solução de storage deve possuir, no mínimo, 192 (cento e noventa e dois) GB de memória cache ECC, somando-se a memória cache de todas as controladoras RAID;

5.5.26.38. A solução de storage deverá permitir a expansão futura com a adição de memória cache ECC, possibilitando a capacidade máxima de 384 (trezentos e oitenta e quatro) GB para a solução;

5.5.26.39. As controladoras devem possuir entre si mecanismo de espelhamento e proteção de cache de escrita de forma a garantir que a integridade e continuidade de funcionamento do storage mesmo com a falha de uma das controladoras;

5.5.26.40. A solução deve incluir suporte a multipathing (múltiplos caminhos) para acesso dos servidores aos discos virtuais criados no storage. O objetivo é oferecer caminhos redundantes entre storages e servidor;

5.5.26.41. A solução de armazenamento deve possuir uma ferramenta nativa do próprio sistema operacional para permitir a integração e gerenciamento dos dados para plataformas de nuvem (cloud) públicas. A ferramenta deve ser capaz de prover funcionalidades conhecidas como Cloud Tiering, Cloud Cache e Cloud Replication para no mínimo as seguintes plataformas: Microsot Azure, Amazon S3 e Google Cloud;

5.5.26.42. Caso a solução ofertada não suporta a integração nativa com cloud exigida no item anterior, deverá ser fornecida uma volumetria adicional de 100% da capacidade de armazenamento.

5.5.27. RENOVAÇÃO SOLUÇÃO DE BACKUP E REPLICAÇÃO DE DADOS:

5.5.27.1. Deverá ser fornecida renovação da solução de backup e replicação de dados pelo período de 36 (trinta e seis) meses para 50 (cinquenta) servidores físicos e virtuais, conforme características técnicas mínimas abaixo:

5.5.27.1.1. Serviço de backup e replicação de dados para ambiente seguro de forma remota para equipamentos servidores e dados, onde as cópias de segurança são armazenadas localmente e em datacenter remoto de forma CRIPTOGRAFADA;

5.5.27.2. A solução deverá incluir funcionalidades de backup e replicação integradas em uma única solução, incluindo retorno (rollback) de réplicas e replicação desde e até a infraestrutura virtualizada;

5.5.27.3. As licenças de software, direitos de atualização e certificados de suporte do fabricante deverão ser entregues ativados e vinculados à Contratante com vigência de 36 (trinta e seis) meses, mantendo-se a eficácia e exigibilidade dessas obrigações perante o fabricante e a integradora credenciada inO licenciamento deverá ser fornecido para a proteção de todo ambiente em produção, durante o período de vigência do contrato, além de suporte e atualização da solução;

5.5.27.4. A solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais;

5.5.27.5. Deverá poder realizar proteção sem parar as máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção e migrações em conjunto;

5.5.27.6. Deverá ser capaz de compreender as máquinas virtuais como objetos do ambiente virtual e proteger as configurações das mesmas, independentemente dos dados da máquina virtual;

5.5.27.7. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual;

5.5.27.8. Deverá prover uma ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador;

5.5.27.9. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais;

5.5.27.10. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos;

5.5.27.11. O serviço de replicação fornecido deverá suportar de forma nativa e realizar regularmente, na frequência definida pela CONTRATANTE, com certificação TIER III, localizado em território nacional;

5.5.27.12. Para fins de segurança da informação os dados deverão ser replicados entre 02 (dois) datacenters, com no mínimo 40 Km de distância entre eles. Em caso de desastre no datacenter principal o ambiente deverá estar disponível do datacenter réplica;

5.5.27.13. O repositório para a cópia da réplica deverá ser disponibilizado com no mínimo 60 TB (Terabytes), disponíveis para armazenamento, sem considerar eventuais ganhos com compressão e duplicação;

5.5.27.14. O repositório externo deverá ser entregue através de integração nativa, via object storage, compatível com o protocolo S3, ou via conectividade nativa da solução de backup, não sendo permitidas soluções de softwares com conexão VPN de terceiros nem integração do repositório via SMB/CIFS;

5.5.27.15. A CONTRATANTE poderá solicitar, a seu critério, testes trimestrais de recuperação de dados do repositório externo (restore) de todos os dados armazenados, a fim de garantir a integridade dos dados copiados;

5.5.27.16. A CONTRATADA deverá disponibilizar até 64 (sessenta e quatro) endereços de IP fixos e públicos (válidos), para uso em ambiente de produção;

5.5.27.17. Em caso de manutenções técnicas programadas por períodos acima de 48h, a CONTRATANTE deverá disponibilizar datacenter virtual, instalado em um datacenter padrão, tier 3, em território brasileiro, a fim de garantir a disponibilidade operacionais e de infraestrutura, limitados a 05 (cinco) máquinas virtuais, ou consumo de 20 vCPU e 40 GB de Memória, 2 TB SSD, 3 TB NL SAS e 10 TB em object storage, durante o período que for necessário para retomar a operação no datacenter principal. A conectividade entre os ambientes será de responsabilidade da CONTRATADA e não deverá onerar o link do ambiente local;

5.5.27.18. A fim de garantir uma conexão de dados com baixa latência e de forma redundante, o licitante deverá comprovar a conexão direta de no mínimo dois pontos de troca de tráfegos distintos (IX' s), em território brasileiro;

5.5.27.19. A fim de garantir que o endereçamento IP utilizado pelo serviço de replicação de backup e recuperação não sofra constantes alterações e consequentes indisponibilidades, a CONTRATADA deverá comprovar durante a fase habilitação que possui seu próprio bloco de endereçamento IP (ASN), atribuído pelo órgão gestor dos serviços de numeração brasileira (NIC.br);

5.5.27.20. Por envolver a prestação de serviços de telecomunicações, a empresa licitante deverá comprovar que possui autorização vigente emitida pela Agência Nacional de Telecomunicações

(Anatel), conforme previsto no art. 131 da Lei 9.472/1997 e no art. 4º da Resolução 777/2025. Para fins de habilitação, será exigida a comprovação de autorização para exploração de serviço de telecomunicações de interesse coletivo e restrito — mediante apresentação do instrumento de outorga ou por consulta pública ao painel “Outorga e Licenciamento” da Anatel (https://informacoes.anatel.gov.br/paineis/outorga-e-licenciamento), sob pena de desclassificação de sua proposta;

5.5.27.21. O ambiente de infraestrutura e sustentação do datacenter virtual, deverá ser entregue e configurado no momento da instalação da Solução de Replicação;

5.5.27.22. Deverá ser provido ferramenta web para análise e geração de relatórios com informações de consumo e status das tarefas off-site;

5.5.27.23. Deverá incluir um plug-in para VMware vSphere Web Client e permitir monitorar a infraestrutura de backup diretamente do vSphere Web Client, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup;

5.5.27.24. Deverá suportar as últimas versões disponíveis dos hypervisors VMware vSphere 7, e superiores, bem como, Microsoft Hyper-V 2012 R2, e superiores;

5.5.27.25. Deverá ter a capacidade de monitoramento em tempo real, sem a necessidade de agentes, da infraestrutura virtual e de backup, inclusive máquinas virtuais, simultaneamente para Hyper-V e VMware, com notificação de problemas de backup e desempenho, com geração de alertas e base de conhecimento embutida para resolução dos mesmos;

5.5.27.26. Deverá ter a capacidade de monitoramento e análise de capacidade do ambiente para crescimento, e ajustes de crescimento;

5.5.27.27. Não deverá requerer licenças independentes para o backup e recuperação granular assistida e consistente de softwares;

5.5.27.28. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados;

5.5.27.29. Deverá permitir um método de fácil recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência;

5.5.27.30. Deverá oferecer a possibilidade de armazenar os arquivos replicados de forma criptografada, assim como assegurar o trânsito da informação através desse cenário;

5.5.27.31. Deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de backup que esteja alojado em um provedor de serviços na nuvem;

5.5.27.32. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:

5.5.27.32.1. Relatórios que permitam o planejamento de capacidade;

5.5.27.32.2. Relatórios que permitam determinar a ineficiência dos recursos em uso;

5.5.27.32.3. Relatórios que facilitem a visibilidade de tendências negativas e anomalias;

5.5.27.32.4. Quadros de controle claros, apresentáveis e integráveis em sites web;

5.5.27.32.5. Deverá permitir a capacidade de gerar segregação de acesso segundo o perfil de um usuário, ao monitoramento da infraestrutura conectada à plataforma;

5.5.27.32.6. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual;

5.5.27.32.7. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos;

5.5.27.32.8. Deverá possuir base de conhecimento integrada aos alarmes, mas também deve suportar a personalização dos alarmes e descrições da base de conhecimento.

5.5.28. SOLUÇÃO DE SEGURANÇA PARA DADOS

5.5.28.1. A solução deverá suportar throughput (Taxa de Transferência) de, no mínimo, 17 Gbps com a funcionalidade de firewall habilitada, independentemente do tamanho dos pacotes;

5.5.28.2. A solução deve suportar Throughput (Taxa de Transferência) de, no mínimo, 0.9 Gbps, com as seguintes funcionalidades habilitadas simultaneamente: Firewall, Controle de Aplicação e Prevenção de Ameaças (Anti Malware, IPS, Application Control URL Filtering). Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;

5.5.28.3. Suportar throughput (Taxa de Transferência) de, no mínimo, 1 Gbps de VPN IPsec;

5.5.28.4. Deverá suportar e incluir licenciamento para, no mínimo, 500 Túneis VPN Lan-to-Lan (ou Gateway-to Gateway), com VPN IPSec;

5.5.28.5. Deverá suportar e incluir licenciamento para, no mínimo, 2.000 usuários remotos (ou client-to-site), com VPN IPSec;

5.5.28.6. Deverá suportar e incluir licenciamento para, no mínimo, 500 usuários remotos (ou client-to-site), com VPN SSL;

5.5.28.7. Suportar no mínimo, 3.500.000 (três milhões e quinhentos mil), conexões TCP simultâneas;

5.5.28.8. Suportar no mínimo, 150.000 (cento e cinquenta mil) novas conexões TCP por segundo;

5.5.28.9. A solução deve possuir o licenciamento para, no mínimo, 10 (dez) sistemas virtuais lógicos (Contextos), independentes entre si e estar licenciado e/ou ter incluído sem custo adicional pelo menos 05 (cinco) sistemas;

5.5.28.10. A solução deve possuir, no mínimo, 02 (duas) interfaces no padrão, 10 GbE (Dez Gigabit Ethernet);

5.5.28.11. A solução deve possuir, no mínimo, 08 (oito) interfaces no padrão 1GbE (Gigabit Ethernet ou 1 Gigabit Ethernet);

5.5.28.12. (CLI);

5.5.28.13. A solução deve possuir console para configuração e gerenciamento por interface de linha de comando. Todas as portas de comunicação e interfaces devem ser capazes de funcionar simultaneamente oferecendo, cada uma, a plenitude de suas capacidades;

5.5.28.14. A solução deve apresentar armazenamento do tipo SSD (Solid-State Drive), com no mínimo 480GB;

5.5.28.15. A solução deve consistir em plataforma para centralização do gerenciamento, dos logs e geração de relatórios dos equipamentos que compõem a solução de segurança rede (NGFW);

5.5.28.16. A solução de gerenciamento, logs e relatório deve ser do mesmo fabricante da solução de segurança de rede (NGFW);

5.5.28.17. As funcionalidades de centralização do gerenciamento, dos logs e geração de relatórios que compõe a plataforma, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

5.5.28.18. Funcionalidades gerais para cluster de equipamentos;

5.5.28.19. Funcionalidades gerais para Solução de Segurança de Perímetro (NGFW);

5.5.28.20. Funcionalidades Gerais e Recursos mínimos:

5.5.28.20.1. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

5.5.28.20.2. Deve suportar o protocolo padrão da indústria VXLAN;

5.5.28.20.3. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

5.5.28.20.4. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing (PBR) ou policy based forwarding (PBF);

5.5.28.20.5. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

5.5.28.20.6. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

5.5.28.20.7. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

5.5.28.20.8. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

5.5.28.20.9. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

5.5.28.20.10. Deve suportar NAT dinâmico (Many-to-1);

5.5.28.20.11. Deve suportar NAT dinâmico (Many-to-Many);

5.5.28.20.12. Deve suportar NAT estático (1-to-1);

5.5.28.20.13. Deve suportar NAT estático (Many-to-Many);

5.5.28.20.14. Deve suportar NAT estático bidirecional 1-to-1;

5.5.28.20.15. Deve suportar Tradução de porta (PAT);

5.5.28.20.16. Deve suportar NAT de Origem;

5.5.28.20.17. Deve suportar NAT de Destino;

5.5.28.20.18. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

5.5.28.20.19. Deve poder combinar NAT de origem e NAT de destino na mesma politica;

5.5.28.20.20. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

5.5.28.20.21. Deve suportar NAT64 e NAT46;

5.5.28.20.22. Deve implementar Equal-cost Multipath ECMP;

5.5.28.20.23. Deve suportar nativamente ou integração com soluções de SD-WAN;

5.5.28.20.24. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

5.5.28.20.25. Deve suportar o padrão do protocolo 'syslog' para geração e armazenamento dos logs usando o formato Common Event Format (CEF);

5.5.28.20.26. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);

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

5.5.28.20.28. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

5.5.28.20.29. Implementar Proteção anti-spoofing;

5.5.28.20.30. Deve identificar e bloquear comunicação com redes botnets;

5.5.28.20.31. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle;

5.5.28.20.32. Deve possuir integração com LDAP para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle;

5.5.28.20.33. Deve possuir integração com Radius para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle;

5.5.28.20.34. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

5.5.28.20.35. Deve possuir funcionalidade de Single Sign-On. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede;

5.5.28.20.36. Deve possuir funcionalidade de Captive Portal local para autenticação de usuários que solicitem navegação através de políticas de firewall que façam o controle por usuários/grupos de usuários;

5.5.28.20.37. 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;

5.5.28.20.38. Deve permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado o acesso à internet e gerenciamento da solução;

5.5.28.20.39. Deve prover nativamente, no mínimo, licenciamento de uso de 01 (um) token, possibilitando autenticação de duplo fator para usuário administrador, acesso VPN etc;

5.5.28.20.40. Para IPv4, deve suportar roteamento estático e dinâmico (RIP, BGP e OSPF);

5.5.28.20.41. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF e BGP);

5.5.28.20.42. Suportar OSPF graceful restart;

5.5.28.20.43. Os dispositivos de proteção devem 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 02 (L2) e camada 03 (L3);

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

5.5.28.20.45. Deve suportar Modo Camada – 02 (L2), para inspeção de dados em linha e visibilidade do tráfego;

5.5.28.20.46. Deve suportar Modo Camada – 03 (L3), para inspeção de dados em linha e visibilidade do tráfego;

5.5.28.20.47. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

5.5.28.20.48. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

5.5.28.20.49. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

5.5.28.20.50. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

5.5.28.20.51. A configuração em alta disponibilidade deve sincronizar: Sessões;

5.5.28.20.52. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

5.5.28.20.53. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

5.5.28.20.54. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

5.5.28.20.55. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

5.5.28.20.56. Deve possuir suporte à criação de sistemas virtuais lógicos (contexto) no mesmo appliance;

5.5.28.20.57. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

5.5.28.20.58. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

5.5.28.20.59. Controle, inspeção e decriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

5.5.28.20.60. Deverá suportar controles por zona de segurança;

5.5.28.20.61. Controles de políticas por porta e protocolo;

5.5.28.20.62. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

5.5.28.20.63. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

5.5.28.20.64. Firewall deve ser capaz de aplicar a inspeção de camada 7 (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

5.5.28.20.65. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

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

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

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

5.5.28.20.69. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

5.5.28.20.70. Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado (s) País/Países, sejam bloqueados;

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

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

5.5.28.20.73. O gerenciamento da solução deve suportar acesso via interface WEB (HTTPS) e interface de linha de comando (SSH), incluindo, mas não limitado à exportar configuração dos sistemas virtuais lógicos por ambas interfaces.

5.5.29. CONTROLE DE APLICAÇÕES:

5.5.29.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

5.5.29.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

5.5.29.3. Reconhecer pelo menos 1500 (mil e quinhentas) 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;

5.5.29.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, 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;

5.5.29.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

5.5.29.6. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

5.5.29.7. 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 utilização da rede Tor;

5.5.29.8. 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;

5.5.29.9. 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 especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

5.5.29.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

5.5.29.11. Atualizar a base de assinaturas de aplicações automaticamente;

5.5.29.12. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

5.5.29.13. 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;

5.5.29.14. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

5.5.29.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

5.5.29.16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

5.5.29.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

5.5.29.18. 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: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

5.5.29.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

5.5.29.20. Deve alertar o usuário quando uma aplicação for bloqueada;

5.5.29.21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

5.5.29.22. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc), possuindo granularidade de controle/políticas para os mesmos;

5.5.29.23. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

5.5.29.24. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

5.5.29.25. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

5.5.29.26. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

5.5.29.27. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

5.5.30. PREVENÇÃO DE AMEAÇAS:

5.5.30.1. 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;

5.5.30.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

5.5.30.3. 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;

5.5.30.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

5.5.30.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo, e enviar tcp-reset;

5.5.30.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

5.5.30.7. 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;

5.5.30.8. Deve permitir o bloqueio de vulnerabilidades;

5.5.30.9. Deve permitir o bloqueio de exploits conhecidos;

5.5.30.10. Deve incluir proteção contra-ataques de negação de serviços;

5.5.30.11. Deverá possuir os seguintes mecanismos de inspeção de IPS:

5.5.30.12. Análise de padrões de estado de conexões;

5.5.30.13. Análise de decodificação de protocolo;

5.5.30.14. Análise para detecção de anomalias de protocolo;

5.5.30.15. Análise heurística;

5.5.30.16. IP Defragmentation;

5.5.30.17. Remontagem de pacotes de TCP;

5.5.30.18. Bloqueio de pacotes malformados;

5.5.30.19. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood;

5.5.30.20. Detectar e bloquear a origem de portscans;

5.5.30.21. Bloquear ataques efetuados por worms conhecidos;

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

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

5.5.30.24. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica;

5.5.30.25. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti spyware, permitindo a criação de exceções com granularidade nas configurações;

5.5.30.26. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

5.5.30.27. Identificar e bloquear comunicação com botnets;

5.5.30.28. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo 24 de 48 dispositivo;

5.5.30.29. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

5.5.30.30. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

5.5.30.31. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

5.5.30.32. Os eventos devem identificar o país de onde partiu a ameaça;

5.5.30.33. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

5.5.30.34. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

5.5.30.35. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseada em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

5.5.30.36. Fornecer proteção contra-ataques de dia zero por meio de estreita integração com os componentes Sandbox (on-premise ou nuvem);

5.5.30.37. Filtro de URL;

5.5.30.38. 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);

5.5.30.39. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

5.5.30.40. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

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

5.5.30.42. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs; **5.5.30.43** Possuir pelo menos 50 categorias de URLs;

5.5.30.44. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

5.5.30.45. Permitir a customização de página de bloqueio;

5.5.30.46. Permitir 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);

5.5.30.47. Além do Explicit Web Proxy, suportar proxy Web transparente;

5.5.30.48. QoS e Traffic Shaping;

5.5.30.49. 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 a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

5.5.30.50. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

5.5.30.51. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

5.5.30.52. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

5.5.30.53. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube;

5.5.30.54. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

5.5.30.55. Possibilitar a definição de tráfego com banda garantida;

5.5.30.56. Possibilitar a definição de tráfego com banda máxima;

5.5.30.57. Possibilitar a definição de fila de prioridade;

5.5.30.58. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

5.5.30.59. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

5.5.30.60. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

5.5.30.61. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

5.5.30.62. VPN;

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

5.5.30.64. Suportar IPSec VPN e VPN SSL de forma simultânea;

5.5.30.65. A VPN IPSEC deve suportar 3DES;

5.5.30.66. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;

5.5.30.67. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

5.5.30.68. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

5.5.30.69. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

5.5.30.70. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;

5.5.30.71. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

5.5.30.72. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

5.5.30.73. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

5.5.30.74. 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;

5.5.30.75. Atribuição de DNS nos clientes remotos de VPN;

5.5.30.76. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

5.5.30.77. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

5.5.30.78. Suportar leitura e verificação de CRL (certificate revocation list);

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

5.5.30.80. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas:

5.5.30.81.1. Antes do usuário autenticar na estação;

5.5.30.81.2. Após autenticação do usuário na estação;

5.5.30.81.3. Sob demanda do usuário;

5.5.30.81.4. Deverá manter uma conexão segura com o portal durante a sessão;

5.5.30.81.5. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

5.5.30.81.6. A demanda do órgão tem como base as seguintes características:

5.5.30.81.7. Composição global da solução estruturada em **Lote Único***;*

5.5.30.81.8. Estratégia de engenharia sob o conceito de **retrofitting tecnológico.**

5.6. ESPECIFICAÇÃO DA GARANTIA DO SERVIÇO

5.6.1. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo 36 (trinta e seis) meses, contado a partir do 1º (primeiro) dia útil subsequente à data do recebimento definitivo do objeto.

5.6.2. A garantia abrange a manutenção corretiva dos bens e a correção de vícios, falhas ou erros decorrentes dos serviços prestados pelo Contratado, mantendo a solução em perfeitas condições de uso e operação, sem qualquer ônus para o Contratante.

5.6.3. Durante o período de reparo, o Contratado deverá disponibilizar equipamento equivalente, peças, insumos e licenças originais e de primeiro uso, ou superior, e os defeitos apresentados deverão ser corrigidos mediante substituição por itens com qualidade igual ou superior aos substituídos.

5.6.4. A reparação ou substituição ocorrerá em até 05 (cinco) dias úteis após a retirada do equipamento ou notificação, prorrogável uma única vez por igual período, mediante solicitação justificada e aceita pelo Contratante.

5.6.5. Os custos referentes ao transporte dos equipamentos em garantia serão de responsabilidade do Contratado.

5.7. PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

5.7.1. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

6. MODELO DE GESTÃO DO CONTRATO

6.1.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei Federal nº 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.1.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.1.3. As comunicações entre o Contratante e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica (e-mail institucional ou sistema oficial) para esse fim.

6.1.4. O Contratante poderá convocar representante do Contratado para adoção de providências que devam ser cumpridas de imediato.

6.1.5. Após a celebração da contratação, o Contratante poderá convocar o representante do Contratado para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do Contratado, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.2. Preposto:

6.2.1. O Contratado designará formalmente o seu preposto antes do início da prestação dos serviços, indicando no instrumento de indicação os poderes e deveres em relação à execução do objeto contratado.

6.2.2. O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto do Contratado, hipótese em que o Contratado designará outro para o exercício da atividade.

6.3. Fiscalização:

6.3.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelo(s) respectivo(s) substituto(s) (Lei nº 14.133, de 2021, art. 117, *caput*).

6.4. Da Fiscalização Técnica:

6.4.1. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração (Decreto estadual nº 68.220, de 2023, art. 17).

6.4.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133, de 2021, art. 117, § 1º e Decreto estadual nº 68.220, de 2023, art. 17, inciso II).

6.4.3. O fiscal técnico realizará, em conformidade com cronograma físico-financeiro, as medições dos serviços executados e aprovará a planilha de medição emitida pelo Contratado (Decreto estadual nº 68.220, de 2023, art. 17, inciso III).

6.4.4. O fiscal técnico adotará medidas preventivas de controle de contratos, manifestando-se quanto à necessidade de suspensão da execução do objeto (Decreto estadual nº 68.220, de 2023, art. 17, inciso IV).

6.4.5. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso (Lei federal nº 14.133, de 2021, art. 117, § 2º).

6.4.6. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato (Decreto estadual nº 68.220, de 2023, art. 17, inciso II).

6.5. Da Fiscalização Administrativa:

6.5.1. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Decreto estadual nº 68.220, de 2023, art. 18, incisos II e III).

6.5.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência (Decreto estadual nº 68.220, de 2023, art. 18, inciso IV).

6.5.3. Sempre que solicitado pelo Contratante, o Contratado deverá comprovar o cumprimento da reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, indicando os empregados alocados, nos termos do parágrafo único do artigo 116 da Lei Federal nº 14.133/2021.

6.6. Da Gestão do Contrato:

6.6.1. O gestor do contrato exercerá a atividade de coordenação dos atos de fiscalização técnica, administrativa e setorial e dos atos preparatórios à instrução processual visando, entre outros, à prorrogação, à alteração, ao reequilíbrio, ao pagamento, à eventual aplicação de sanções e extinção do contrato (Decreto estadual nº 68.220, de 2023, inciso III do art. 2º).

6.6.2. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais (Decreto estadual nº 68.220, de 2023, art. 16, inciso IX).

6.6.3. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações (Decreto estadual nº 68.220, de 2023, art. 16, inciso VI).

6.6.4. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso (Decreto estadual nº 68.220, de 2023, art. 16, inciso VIII).

6.6.5. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração (Decreto estadual nº 68.220, de 2023, art. 16, inciso VII e parágrafo único).

6.6.6. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. CRITÉRIO DE MEDIÇÃO E PAGAMENTO

7. CRITÉRIO DE MEDIÇÃO E PAGAMENTO

7.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), para aferição da qualidade da prestação dos serviços.

7.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que o Contratado:

7.1.1.1. não tenha produzido os resultados acordados,

7.1.1.2. tenha deixado de executar as atividades contratadas, ou não as tenha executado com a qualidade mínima exigida; ou

7.1.1.3. tenha deixado de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os tenha utilizado com qualidade ou quantidade inferior à demandada.

7.2. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

7.3. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

7.3.1. cumprimento dos prazos estabelecidos no cronograma aprovado pela Administração;
7.3.2. entrega integral dos equipamentos previstos;
7.3.3. instalação física dos equipamentos;
7.3.4. configuração lógica da solução;
7.3.5. funcionamento integral da solução;
7.3.6. entrega da documentação técnica e termos de garantia;

7.4. DO RECEBIMENTO

7.4.1. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelo fiscal técnico e administrativo, mediante termo detalhado, quando verificado o cumprimento das exigências de caráter técnico e administrativo (Art. 140, I, "a", da Lei nº 14.133, de 2021 e arts. 17, X, e 18, VI, do Decreto estadual nº 68.220, de 2023).

7.4.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se refere a parcela a ser paga.

7.4.3. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico (Art. 17, X, Decreto estadual nº 68.220, de 2023).

7.4.4. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo (Art. 18, VI, Decreto estadual nº 68.220, de 2023).

7.4.5. O fiscal setorial do contrato, when houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

7.4.6. Para efeito de recebimento provisório, ao final de cada período de faturamento, que observará as regras contratuais, o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos ao Contratado, registrando em relatório a ser encaminhado ao gestor do contrato.

7.4.6.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

7.4.6.2. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.4.6.3. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório (Art. 119 c/c art. 140 da Lei nº 14.133, de 2021).

7.4.6.4. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos manuais e instruções exigíveis.

7.4.6.5. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades cabíveis.

7.4.7. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.4.8. Os serviços serão recebidos definitivamente no prazo de até 60 (sessenta) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo aos seguintes procedimentos:

7.4.8.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao

seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (Decreto estadual nº 68.220, de 2023, art. 16, inciso VI);

7.4.8.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando ao Contratado, por escrito, as respectivas correções;

7.4.8.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

7.4.8.4. Comunicar ao Contratado para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização; e

7.4.8.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.4.9. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, se houver parcela incontroversa, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, com a comunicação ao Contratado para emissão de Nota Fiscal no que pertine à parcela incontroversa, para efeito de liquidação e pagamento.

7.4.10. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo Contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.4.11. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.5. LIQUIDAÇÃO

7.5.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, a contar de seu recebimento pela Administração, na forma desta seção, prorrogáveis por igual período, justificadamente, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais (art. 7º, I, e §§ 2º e 3º, da Instrução Normativa SEGES/ME nº 77, de 4 de novembro de 2022, c/c o Decreto estadual nº 67.608, de 2023).

7.5.2. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como, caso aplicáveis:
7.5.2.1. o prazo de validade;
7.5.2.2. a data da emissão;
7.5.2.3. os dados do contrato e do órgão contratante;
7.5.2.4. o período respectivo de execução do contrato;
7.5.2.5. o valor a pagar; e
7.5.2.6. eventual destaque do valor de retenções tributárias cabíveis.

7.5.3. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

7.5.4. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao Sicaf ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.5.5. A Administração deverá realizar consulta ao Sicaf para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, tais como proibição de contratar com o Poder Público, bem como

ocorrências impeditivas indiretas (Instrução Normativa SEGES/MPDG nº 3, de 26 de abril de 2018, c/c Decreto estadual nº 67.608, de 2023).

7.5.5.1. Constatando-se, junto ao Sicaf, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defense. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

7.5.5.2. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.5.5.3. Persistindo a irregularidade, o Contratante deverá adoptar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

7.5.5.4. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso o Contratado não regularize sua situação junto ao Sicaf.

7.6. PRAZO DE PAGAMENTO

7.6.1. O pagamento será efetuado no prazo de 30 (trinta) dias, contados da apresentação da nota fiscal ou documento de cobrança equivalente, desde que tenha sido finalizada a liquidação da despesa, conforme seção anterior, nos termos do art. 2º, inciso II, do Decreto estadual nº 67.608, de 2023.

7.6.2. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente na forma da legislação aplicável (art. 2º, inciso III, do Decreto estadual nº 67.608, de 2023, c/c o art. 1º do Decreto estadual nº 32.117, de 1990), bem como incidirão juros moratórios, **à razão de** 0,5% (meio por cento) ao mês, calculados *pro rata temporis*, em relação ao atraso verificado.

7.7. FORMA DE PAGAMENTO

7.7.1. O pagamento será realizado por meio de ordem bancária, para depósito em conta corrente bancária em nome do Contratado no Banco do Brasil S/A.

7.7.2. Constitui condição para a realização dos pagamentos a inexistência de registros em nome do Contratado no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pelo Contratado, de que os registros estão suspensos, nos termos do art. 8º da Lei estadual nº 12.799, de 2008.

7.7.3. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.7.4. O Contratante poderá, por ocasião do pagamento, efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

7.7.5. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8. SELEÇÃO DO FORNECEDOR E EXECUÇÃO

8.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade pregão, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

8.1.2. O regime de execução do contrato será empreitada por preço global.

8.2. Exigências de habilitação

8.2.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos das seções subsequentes deste item 8, que serão exigidos conforme sua natureza jurídica:

8.2.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.2.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.2.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

8.2.1.4. Sociedade empresária: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.2.1.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME nº 77, de 18 de março de 2020;

8.2.1.6. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.2.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

8.2.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

8.3. Habilitação fiscal, social e trabalhista

8.3.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

8.3.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente aos créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

8.3.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.3.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.3.5. Prova de inscrição no cadastro de contribuintes Estadual/Distrital e/ou Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.3.6. Prova de regularidade com a Fazenda Estadual/Distrital nos termos da Lei Complementar nº 214, de 2025, quanto ao Imposto sobre Bens e Serviços – IBS, e/ou de regularidade com a Fazenda Municipal/Distrital quanto ao Imposto sobre Serviços de Qualquer Natureza - ISSQN, do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.3.7. Caso o fornecedor se considere isento ou imune de tributos relacionados ao objeto contratual, em relação aos quais seja exigida regularidade fiscal neste instrumento, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8.4. Qualificação econômico-financeira

8.4.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021 c/c Decreto estadual nº 67.608, de 2023), ou de sociedade simples;

8.4.2. Certidão negativa de falência, expedida pelo distribuidor da sede do fornecedor, caso se trate de empresário individual ou sociedade empresária;

8.5. Qualificação Técnica

8.5.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

8.6. Outras Comprovações

8.6.1. Declaração subscrita por representante legal do licitante, atestando que:

a) cumpre as normas relativas à saúde e segurança no trabalho, nos termos do art. 117, parágrafo único, da Constituição Estadual;

b) atenderá, na data da contratação, ao disposto no art. 5º-C e se compromete a não disponibilizar empregado que incorra na vedação prevista no art. 5º-D, ambos da Lei nº 6.019, de 1974, com redação dada pela Lei nº 13.467, de 2017, quando o caso.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O valor estimado total da contratação é de **R$ 5.895.300,00 (cinco milhões oitocentos e noventa e cinco mil e trezentos reais),** conforme custos unitários apostos. O valor estimado da contratação foi definido com observância do disposto no Decreto estadual nº 67.888, de 17 de agosto de 2023.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do Estado.

10.2. No presente exercício, a contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: 00001/ 180184;

II) Fonte de Recursos: 150010001 - FISP;

III) Programa de Trabalho: 180433 - Muralha Paulista;

IV) Elemento de Despesa: 33904017.

10.3. Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao exercício financeiro subsequente será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

PEDRO RANGEL SILVA

Chefe de Seção

Assinou eletronicamente em 17/09/2026 às 08:25:18.