Especificação técnica de infraestrutura de rede de CFTV digital no Centro de Controle

1. Esta Especificação destina-se a orientar as linhas gerais para o fornecimento de equipamentos. Devido às especificidades de cada central e de cada aplicação, todos os itens desta Especificação estão sujeitos a revisões, que podem implicar em alterações, acréscimos ou exclusões. Portanto, a aplicação desta Especificação não deverá ser automática, devendo sempre ser submetida à análise das áreas envolvidas antes da efetivação do fornecimento.

1.1. Caso o fornecedor/instalador não seja o fabricante dos equipamentos que irá fornecer, deverá ser certificado por este como revendedor, integrador ou distribuidor autorizado.

1.2. O fabricante dos equipamentos a serem fornecidos deverá possuir instalações próprias de suporte técnico permanente no Brasil.

2. Os elementos básicos que comporão a rede são:

- Servidor de vídeo em rede
- *Data storage*
- Estações de trabalho
- *Video wall*
- Switches e roteadores
- Softwares de gerenciamento de vídeo e de rede
- Infraestrutura e cabeamento

3. A rede TCP/IP deverá garantir a segurança e a inviolabilidade das informações que trafegarem através da rede por intermédio da aplicação de mecanismos de criptografia na comunicação, firewall e software antivírus.

4. Deverá possuir dispositivos que impeçam o acesso de pessoas não autorizadas à rede, às câmeras e a quaisquer outros equipamentos que possam comprometer a integridade das informações e as funcionalidades do subsistema.

5. Comunicação entre switch, servidor de vídeo e data storage deverá ser por meio de fibra óptica.

6. A rede e os equipamentos que a compõem deverão ser dimensionados para operar todas as câmeras simultaneamente, em formatos de compressão H.264 e M-JPEG, resolução megapixel (1280 x 800 pixels), a 30 fps.

7. Deverão ser fornecidos os softwares de proteção antivírus e firewall com licenças de atualização pelo período mínimo de 2 anos para todos os computadores e estações de trabalho fornecidas.

8. Servidor de vídeo:

8.1. O servidor de vídeo terá a finalidade de controlar todas as operações relacionadas às câmeras de CFTV, novas ou existentes, fixas ou PTZ, como monitoramento, telecomando, gravação e recuperação de imagens.

8.2. Deverá ter a capacidade de processar os dados que trafegam na rede e acessar o data storage como um único equipamento de armazenamento, ainda que seja composto de várias unidades.

8.3. O número de servidores requeridos para o desempenho das funções necessárias da Central de Operações será definido pela CET na época da implantação.

8.4. **Gabinete:**

- Tipo rack padrão 19 polegadas com altura de 2U com trilhos e quaisquer outros componentes necessários para instalação em rack ofertados como padrão do produto;
- Deve possuir fontes redundantes hot-plug ou hot-swap;
- Deve possuir ventiladores redundantes hot-plug ou hot-swap;
- Deve possuir display de LEDs acoplados no painel frontal do servidor para indicar e monitorar as condições de funcionamento;
- Deve possuir painel frontal de proteção do servidor com chave, para evitar acesso físico indevido aos discos do equipamento.

8.5. **Processador:**

- O servidor deve possuir 2 processadores com tecnologia 8-Core ou superior, originalmente desenvolvido para servidores, com frequência de clock de, no mínimo, 2.90GHz.
- O servidor deve possuir chipset desenvolvido para arquitetura de servidores, sendo ele do fabricante do processador.

- Padrão de arquitetura do processador x86 de 32 bits com suporte a extensão 64 bits, com tecnologia de fabricação de 32 nanômetros e memória cache L3 integrada ao processador de no mínimo 20MB.
- A velocidade do barramento de comunicação do processador com o restante do sistema deverá ser de no mínimo 8GT/s (gigatransfers por segundo).
- O processador deve implementar mecanismos de redução de consumo de energia.

8.6. **Desempenho:**

- O servidor deverá ter índice SPECint_rate_base2006 auditado de no mínimo 515 pontos para dois processadores de tecnologia 8-Core.
- Caso o servidor ofertado não esteja auditado com a quantidade de processador solicitado e/ou com frequência de processador diferente para atingimento da pontuação solicitada, deverá ser aplicada fórmula SPECint_rate_base2006_estimado = (SPECint_rate_base2006_auditado * (clock_processador_servidor_ofertado / clock_processador_servidor_auditado)) / (número de processadores ofertado / número de processadores auditado).
- Não será aceito para cálculo, indice SPECint_rate_base2006 de servidor cuja frequência de clock seja inferior à frequência do clock ofertado.
- Os índices SPECint_rate_base2006 utilizados como referência serão validados junto ao site www.spec.org
- Não serão aceitas estimativas para modelos de servidores não auditados.
- O índice apresentado deverá ser baseado em SPEC auditado para o mesmo modelo da família de servidores (marca e modelo).

8.7. **Memória:**

- Deverão ser fornecidos no mínimo 128GB de memória RAM do tipo RDIMM por servidor.
- Todos os canais de memória deverão possuir pelo menos um módulo de memória com tamanho mínimo de 8GB.
- Deverá suportar expansibilidade de até 384GB com módulos do tipo RDIMM.
- Deverá possuir no mínimo 24 slots do tipo DIMM.
- O chipset deverá suportar memória RAM do tipo DDR3 com frequência de 1600MHz.
- O servidor ofertado deve oferecer suporte aos recursos de Advanced ECC ou similar e online spare ou memory mirroring.

8.8. **BIOS:**

- O BIOS deverá ser do tipo Flash Memory, utilizando memória não volátil e eletricamente reprogramável.
- Deverá mostrar no monitor de vídeo o nome do fabricante do servidor sempre que o servidor for inicializado.

- A inicialização do servidor deverá ser realizada na sequência definida pelo usuário, via CD-ROM e/ou disco rígido, bem como pela placa de rede através do recurso WOL (Wake on LAN).
- Deverão possuir recursos de controle de permissão através de senhas, uma para inicializar o servidor e outra para acesso e alterações das configurações do BIOS.

8.9. **Slots de expansão:**

- O servidor ofertado deverá possuir pelo menos 4 slots PCI-Express, sendo que pelo menos 2 deles sejam do tipo PCI Express 3.0 com conector do tipo X16 e banda de passagem do tipo X8.

8.10. **Portas de comunicação:**

- Todos os conectores das portas de entrada/saída de sinal deverão ser identificados pelos nomes ou símbolos.
- 1 porta serial.
- 2 portas de vídeo padrão DB15.
- 6 portas USB 2.0, sendo pelo menos duas portas livres na parte traseira e outras duas portas dedicadas para teclado e mouse.

8.11. **Interface de rede**

- 4 interfaces de rede Gigabit Ethernet, com suporte aos protocolos , IEEE 802.3, IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x, IEEE 802.3ad, IEEE 802.3az, IEEE 802.1q e IEEE 802.1as.
- Tais interfaces de rede podem ser ofertadas integradas à placa mãe.
- As placas de rede ofertadas devem suportar o recurso de Teaming (NIC teaming).
- Deve possuir o recurso Wake on Lan.
- Deve possuir o recurso PXE.
- Deve possuir suporte a VLAN, Link Aggregation e Jumbo Frames.
- Deve possuir suporte a VMware NetQueue e Microsoft VMQ.

8.12. **Interfaces fibre channel:**

- 2 placas HBA;
- Velocidade que permita 8, 4 e 2 Gbps;
- Mínimo de 1 porta FC com respectivos módulos SFP+ de ondas curtas (short wave);
- Instalada em slot PCI Express com barramento mínimo x8;
- 4 cabos duplex multimodo com comprimento de 5m e conectores LC/LC compatível com as placas integrantes ao servidor.

8.13. **Controladora de vídeo:**

- A placa de vídeo deve permitir a virtualização de hardware da GPU permitindo que a tela do desktop virtual seja enviada diretamente ao protocolo de acesso remoto. Possuir mecanismos de codificação H.264 de alta performance, capaz de codificar fluxos simultâneos com qualidade superior. Deve possuir minimamente 4 GPUs baseadas em tecnologia Kepler e 16 GB de memória dedicada DDR3 compatível com PCIe x16 de 2ª e 3ª gerações. Possuir eficiência energética e compatibilidade com soluções de virtualização de GPU da Citrix, Microsoft e VMware. Altura máxima de 4,4" e solução de resfriamento passiva.
- Resolução gráfica mínima de 1280 x 1024.

8.14. **Controladora de disco rígido (RAID):**

- No mínimo 1 controladora para controle dos discos rígidos.
- Onboard e/ou offboard de acordo com o padrão de slots solicitado.
- Deverá possuir canais suficientes para o controle dos discos rígidos previstos no item 8.15.
- Padrão SAS ou superior.
- Memória cache implementada na controladora com no mínimo 1GB do tipo Flash.
- Taxa de transferência de dados de no mínimo 6Gb/s.
- Deverá possibilitar a implementação dos níveis de RAID 0, 0 + 1 ou 1+0, 1 e 5.
- As funcionalidades de array devem ser implementáveis e configuráveis por hardware através de utilitário específico.

8.15. **Disco rígido:**

- Mínimo de 8 baias hot-plug ou hot-swap disponíveis para discos SAS ou superior.
- No mínimo 4 discos rígidos por servidor.
- Capacidade mínima de armazenamento por disco de 500GB Tipo hot-pluggable de 2.5" (polegadas).
- Velocidade de rotação mínima de 10000 RPM.
- Taxa de transferência de dados de 6Gb/s.
- Tecnologia de pré-falha SMART (Self Monitor Analysis Report Test) ou equivalente incorporado, atrelado à controladora de disco e a software de gerenciamento.

8.16. **Unidade ótica:**

- Deverá possuir 1 unidade de leitura DVD-RW ou Blu-ray por servidor.
- Tipo interno ao gabinete.
- Fonte de alimentação

- O servidor deve possuir fontes de alimentação redundantes e hot-plug ou hot-swap, para substituição automática da fonte de alimentação principal em caso de falha, mantendo assim o seu funcionamento.
- Faixa de tensão de entrada de 100Vac a 240Vac, a 60Hz.
- Cabos de alimentação com plug padrão IEC para ambientes de 220V para cada fonte de alimentação fornecida.
- Deverá possuir eficiência energética de no mínimo 92%.

8.17. **Sistema de ventilação:**

- Deverá possuir ventiladores redundantes hot-plug ou hot-swap, necessários para a refrigeração do sistema interno do servidor na sua configuração máxima.

8.18. **Acesso remoto:**

- O servidor deve oferecer a funcionalidade de acesso remoto ao sistema operacional via browser.
- Permitir boot e reboot remoto.
- Acesso a console com criptografia e segurança padrão SSL, no mínimo.
- Acesso à console gráfica do servidor, mesmo em falha de sistema operacional.
- Definição de senhas e criptografia para clientes remotos.
- Visualização de POST durante a inicialização.
- Permitir a configuração da BIOS.
- Permitir a configuração remota do equipamento através de midia virtual (CD, DVD etc.)
- O equipamento ofertado deve possuir uma porta dedicada, com conector RJ-45, para gerenciamento remoto, não sendo essa interface nenhuma das controladoras de rede especificadas.
- Permitir a criação de, no mínimo, 12 contas de usuários, com customização de privilégios, e/ou a integração à base de usuários existente (Active Directory ou algum outro diretório compatível com LDAP).
- Permitir mínimo de 6 usuários o acesso simultâneo, independente da localização, para melhor gerenciamento do servidor.

8.19. **Qualidade do equipamento:**

- O servidor deve estar em conformidade com a norma IEC 60950 (Safety of Information Technology Equipment Including Eletrical Business Equipment), para segurança do usuário contra incidentes elétricos e combustão dos materiais elétricos.
- O equipamento ofertado deve possuir certificado e estar em conformidade com as normas CISPR22 – Classe A ou FCC – Classe A, para assegurar níveis de emissão eletromagnética.

8.20. **Responsabilidade com o meio ambiente:**

- O modelo ofertado deve estar em conformidade com o padrão RoHS (Restriction of Hazardous Substances), isto é, deve ser construído com materiais que não agridem o meio ambiente.
- O fabricante deve possuir comprovadamente certificação ISO 14001 – Gestão Ambiental.

8.21. **Certificados:**

- Certificação VmWare - O modelo do servidor ofertado deve ser totalmente compatível com o software de virtualização VmWare, na versão mínima vSphere 4 ou superior, através de pesquisa ao link : http://www.vmware.com/resources/compatibility/search.php
- Certificação RedHat - O modelo do servidor ofertado deve constar da lista de equipamentos certificados pela Red Hat, possuindo o Red Hat Hardware Catalog no mínimo na versão 5 ou superior, a pesquisa poderá ser feita através do link: http://hardware.redhat.com/hcl/
- Certificação Suse - O modelo do servidor ofertado deve constar na lista de equipamentos certificados pela Novell Suse, possuindo certificação para no mínimo a versão enterprise 10 ou superior, a pesquisa poderá ser feita através do link: http://developer.novell.com/yessearch/Search.jsp
- Certificação Microsoft - O modelo do servidor ofertado deve constar na lista de equipamentos que possuem Certified Servers for Windows Server 2008 R2 (Certified for Windows - Enhanced Power Management) do Windows Server Catalog, através de pesquisa ao link: http://www.windowsservercatalog.com

8.22. **Itens adicionais:**

- Deverá possuir sensores (hardware) de temperatura e de fonte de energia e estar em condições de exercer monitoramento ativo dessas variáveis.
- Deverá possuir funcionalidade de reinicialização automática do equipamento em caso de falha grave na operação.
- Deverá vir acompanhado de software específico para realizar a instalação do sistema operacional e dos drivers de todos os dispositivos opcionais que o acompanham (do mesmo fabricante do servidor) integrado ao hardware.
- Fornecimento de Sistema Operacional compatível com a solução ofertada.
- Deverá vir acompanhado de software de gerenciamento, do próprio fabricante do equipamento, com integração total entre agentes de hardware, e com as seguintes características:
- Localização e identificação de servidores e desktops tanto do mesmo fabricante quanto de terceiros, através de snmp, dmi, wbem, wmi ou ipmi 2.0.
- Envio de alertas através de e-mail.
- Acesso via console WEB com possibilidade de definição de direitos administrativos.

- Identificação e envio automático de mensagens de alerta em casos de pré-falha de processador, memória e disco rígido.
- Permitir geração de relatórios incluindo: contrato e garantia dos equipamentos, consumo de energia e refrigeração, performance para análise de gargalos e inventário.
- Permitir integração com softwares de gerenciamento de ambientes virtualizados de terceiros, como Microsoft System Center e Vmware Vcenter;
- Possuir a capacidade de visualização da saúde dos servidores físicos e virtuais.
- Possuir a funcionalidade de instalação de imagens de sistemas operacionais de forma automatizada.
- Deverão fornecer junto ao servidor, kit de trilhos e braço metálico retrátil organizador de cabos para fixação dos servidores em racks padrão 19 polegadas, a fim de facilitar a manutenção do equipamento.
- Para fins de comprovação das características técnicas do equipamento deverão ser incluídos na proposta técnica todos os catálogos, folders, manuais ou declarações do fabricante que comprovem todos os itens constantes neste anexo.
- Informar na proposta: marca, modelo e o fabricante do equipamento, bem como, descrever tecnicamente o produto ofertado, sendo ainda necessário apresentar uma lista informando todos os part numbers (códigos dos produtos) dos servidores, peças, acessórios, componentes e serviços contratados com as suas respectivas quantidades.

9. Data storage e armazenamento (gravação) de imagens:

9.1. As imagens captadas pelas câmeras serão armazenadas em equipamento de data storage conectado ao servidor de vídeo da sua Central de Operações por meio da rede de vídeo digital.

9.2. O equipamento de data storage deverá ser interpretado pelo servidor e pela rede TCP/IP como um único equipamento, ainda que seja composto de várias unidades.

9.3. As imagens de todas as câmeras deverão ser gravadas de forma simultânea e contínua, 24 horas por dia.

9.4. O tamanho do storage deverá ser dimensionado para gravar 100 câmeras simultâneas, em formato de compressão H.264, resolução 4CIF (704 x 480 pixels), a 12 fps, pelo período contínuo de 30 dias. Este dimensionamento poderá ser alterado pela CET na época da implantação.

9.5. A gravação deverá ser cíclica, pelo período mínimo de 30 dias, após o qual as imagens mais antigas serão substituídas automaticamente pelas mais recentes.

9.6. **Especificações Técnicas:**

- O Sistema de Armazenamento de Dados deverá atender aos sistemas computacionais existentes de forma integrada, através de um único equipamento conectando simultaneamente esses sistemas computacionais clientes através de uma rede de armazenamento SAN (Storage Area Network) (modo de acesso aos dados: block I/O) e através de uma rede de armazenamento NAS (Network Attached Storage) (modo de acesso aos dados: file I/O);
- Deverá suportar os seguintes protocolos: iSCSI, FCP, CIFS e NFS. Esses protocolos devem estar habilitados para uso nativo, sem adição de equipamentos ou módulos adicionais, para qualquer área do Sistema de Armazenamento de Dados;
- Deverá ser constituído de, pelo menos, um par de controladoras (módulos ou "engines") configurado de forma redundante, sem ponto único de falha, de modo a disponibilizar aos sistemas computacionais clientes, total e pleno acesso a toda a área de armazenamento sem prejuízo de funcionalidade, mesmo em situação de falha de um dos componentes: CPU, memória cache, barramento de dados, fonte de alimentação, sistema de refrigeração ou interfaces de comunicação Ethernet ou Fibre Channel;
- Em caso de falha de alguma controladora ou componente do Sistema de Armazenamento, um componente redundante equivalente deverá assumir automaticamente (failover automático) as funções e as respostas às requisições encaminhadas pelos sistemas computacionais clientes ao componente que falhou.
- As controladoras devem funcionar de modo ATIVO/ATIVO, ou seja, as duas controladoras devem estar em uso simultâneo, independente da rede de armazenamento SAN ou NAS, recebendo ou fornecendo dados;
- Deverá permitir a troca ou substituição das controladoras por controladoras de maior capacidade ou performance, para crescimento ou expansão dos ambientes, sem necessidade de qualquer tipo de migração ou movimentação de dados, mantendo todos os discos existentes, bem como todos os dados neles gravados.
- Deverá permitir a substituição de uma controladora avariada sem a necessidade de formatação e/ou reconfiguração dos raid groups, LUNs ou volumes/partições, mantendo todos os dados existentes nos discos sem a necessidade de nenhum tipo de migração de dados ou interrupção do acesso dos clientes;
- Deverá suportar a instalação de discos dos seguintes tipos abaixo, incluindo a possibilidade de uso simultâneo dos mesmos no sistema:
    - SSD (Solid State Disk) categoria Enterprise;
    - SAS (Serial Attached SCSI) com no mínimo 10.000 RPM;

    - SAS (Serial Attached SCSI) com no mínimo 15.000 RPM;
    - SATA (Serial Advanced Technology Attachment) com no mínimo 7.200 RPM;
- Deverá permitir a utilização de discos de mesmo tipo, com diferentes capacidades de armazenamento, na mesma gaveta de discos;
- Deverá possuir barramentos internos para espelhamento dos dados de escrita entre as controladoras;
- Deverá possuir baterias que garantam a integridade dos dados gravados pelos sistemas computacionais clientes por um período mínimo de 48 horas ou possuir mecanismo de "destaging" que garantam a integridade desses dados gravados;
- Deverá possuir fontes de alimentação, ventiladores, controladoras, discos, gavetas de expansão e baterias redundantes que possibilitem manutenção e atualização sem a necessidade de parada do equipamento ou acesso dos usuários;
- Deverá suportar atualização de microcódigo (firmware) da controladora e discos de modo não disruptivo;
- Deverá permitir a configuração de proteção física de discos através da tecnologia RAID, que garanta a integridade e a disponibilidade dos dados, mesmo no caso de falha de até quaisquer 2 discos de dados no mesmo raidgroup;
- Deverá permitir a troca entre os diferentes tipos de RAID de forma automática sem a necessidade de migração de dados ou parada do ambiente;
- Deverá permitir a inclusão, mesmo unitária, de discos dentro do raidgroup sem nenhum tipo de indisponibilidade do ambiente;
- Deverá possuir monitoramento pró-ativo que permita a detecção e isolamento de falhas antes que elas ocorram. Tal função abrangerá desde automonitoração, geração de log de erros, detecção e isolamento de erros de memória ou dos discos;
- Deverá permitir a troca ou instalação, sem parada (hot swap) de discos de reserva (spare disk). Os discos de reserva devem ser globais (global hot spare) para cada controladora, e a substituição deverá ser automática em caso de falha de qualquer disco em utilização, ou seja, na falha de qualquer disco, este será substituído, automaticamente, e sem necessidade de intervenção manual, por um disco de reserva, sem que seja necessária, posteriormente, qualquer nova movimentação ou cópia de dados. Após a substituição, o disco de reserva passará a ser reconhecido definitivamente como disco de dados;
- Deverá vir acompanhado de todos os manuais necessários para instalação, configuração e operação da solução;
- Deverá ter suporte nativo ao protocolo IPv6 e estar devidamente licenciado;

- Deverá ser fornecido com a funcionalidade de “snapshot”, ou “point-in-time backup”, de quaisquer áreas de dados da solução, implementado através de ponteiros, com capacidade de armazenar, no mínimo, 250 versões por cada volume/partição existente no sistema de armazenamento. Esta funcionalidade deverá ser executada internamente ao sistema de armazenamento, sem consumir ciclo de CPU dos servidores conectados ao objeto deste edital e sem gerar movimentação de dados de nenhum tipo, além de não causar queda de performance da solução ofertada;
- Deverá ser fornecido com a capacidade de recuperação completa de áreas usadas de “snapshot” ou “point-in-time backup”, através de seus ponteiros, por comando administrativo no sistema de armazenamento, sem a necessidade de movimentação ou cópia física dos dados. Deverá ser fornecido o licenciamento (caso seja licenciada) considerando a capacidade máxima de armazenamento da solução de controladoras fornecidas;
- Deverá ser fornecido com a capacidade de criar cópias Clones, totalmente independentes dos dados originais, para cada volume lógico configurado no sistema de armazenamento de dados. Deve ser possível transformar qualquer cópia clone em um novo volume lógico a qualquer momento. O clone deve ser criado a partir de apontadores aos dados originais, não sendo necessária movimentação de dados para sua criação ou existência. Deverá ser fornecido o licenciamento (caso seja licenciada) considerando a capacidade máxima de armazenamento da solução de controladora fornecida.
- Deverão ser fornecidos os softwares/licenças para integração do snapshot da solução ofertada com gerenciadores de bancos de dados Oracle e MS-SQL, com os aplicativos MS-Exchange, MS-SharePoint e com os sistemas operacionais VMware ESX, Microsoft Windows, Microsoft Hyper-V e compatíveis com Linux/Unix, permitindo o agendamento e/ ou execução de clones, restores, replicações e backups diretamento do servidor de aplicação.
- Deverá estar licenciado e implementado com a capacidade de replicação remota de volumes do sistema de armazenamento de dados, para outro sistema de armazenamento de dados, inclusive de forma bidirecional, sobre rede baseada em protocolo IP, nas três formas: Assíncrona, Síncrona ou Semisíncrona. Esta funcionalidade deve ser gerenciável e configurável através da interface de gerência própria do sistema. Deverá possuir capacidade de “failover” e “failback” com sincronização incremental entre sessões de replicação. Deverá possuir a capacidade de controle de banda de rede usada para a replicação. Esta funcionalidade deverá ser executada internamente ao sistema de armazenamento de dados, para qualquer tipo de dado armazenado, sem inclusão de nenhum equipamento adicional e sem consumir ciclo de CPU dos sistemas computacionais dos clientes

conectados ao sistema de armazenamento de dados, devendo estar licenciado sem limite do volume dados replicados;

- Deverá ser fornecido com a capacidade nativa do equipamento para desduplicar os dados gravados no próprio sistema de armazenamento de dados, eliminando dos volumes os blocos de dados iguais. A desduplicação deverá funcionar para qualquer tipo de dado disponível no equipamento, tanto para dados disponibilizados através da rede SAN (blocked-io), quanto da rede NAS (File-io), inclusive para os dados gravados em áreas destinadas a aceleração de leitura ou gravação (Memória Flash ou SSD), se existentes;
- Deverá ser fornecido com a capacidade nativa do equipamento para compressão dos dados gravados no Sistema de Armazenamento de Dados, comprimindo os blocos de dados antes de serem armazenados nos discos. A compressão deverá funcionar para qualquer tipo de dado disponível no equipamento, tanto para dados disponibilizados através de rede SAN, quanto de rede NAS. Para os casos de licenciamento por capacidade, considerar a capacidade máxima de escalabilidade do subsistema de armazenamento ofertado;
- Deverá suportar o provisionamento virtual da capacidade (virtual ou thin provisioning) de volumes lógicos, devendo funcionar para qualquer tipo de dado disponível no equipamento. Deverá estar ativo para todo o equipamento. O sistema deve ter a capacidade de habilitar e desabilitar o ThinProvisioning de forma não desruptiva e instantânea;
- Permitir a alocação da área de armazenamento, a critério do cliente, em qualquer proporção entre as arquiteturas solicitadas, SAN e NAS; isto é, de 100% SAN a 100% NAS, passando por todas as combinações possíveis em passos de 1%;
- Deverá possuir a capacidade de funcionamento com os protocolos: iSCSI e FCP, sendo implementados nativamente no sistema de armazenamento de dados. Esses protocolos deverão estar licenciados e ativados para todo sistema;
- Deverá suportar o protocolo iSCSI para os ambientes operacionais VMware ESX, Red Hat Linux , SuSE Linux e Microsoft Windows via Microsoft-Logo Certified, constando na HCL da Microsoft.
- Deverá incluir mecanismo de LUN Masking, permitindo assim que volumes sejam acessados somente por hosts autorizados;
- Deverá ser fornecido com os protocolos NFS versões 2, 3 e 4 e CIFS versões 1.0 e 2.0. Estes protocolos deverão estar licenciados e ativados para todo sistema, devendo permitir a utilização simultânea, de um mesmo volume/partição. O sistema deve utilizar mecanismos de file-locking seguro entre os ambientes CIFS e NFS, controlando o acesso simultâneo dos dados pelos usuários/aplicações;
- Deverá permitir assumir o papel de servidor de arquivos do ambiente, para clientes NAS sem necessidade de instalação de outros servidores ou quaisquer equipamentos ou controladoras adicionais;

- Suportar o controle de quotas por usuários e pastas, implementado nativamente no sistema, sem necessidade de instalar nenhum produto adicional nos sistemas computacionais dos clientes;
- Integração nativa com Microsoft Windows Active Directory Service do Windows 2000, 2003 e 2008;
- Deverá permitir o redimensionamento (aumento e/ou diminuição) imediato do tamanho dos volumes/partições acessados pelos sistemas computacionais clientes ligados o sistema de armazenamento de dados sem impacto ou reconfiguração para nos clientes;
- Deverá ser fornecido com a funcionalidade de WORM (Write Once Read Many) para retenção de arquivos, impedindo sua exclusão ou modificação antes de expirado o período de retenção configurado. Deverá implementar relógio interno protegido contra fraude ou alteração manual do período de retenção. A funcionalidade deverá permitir a escolha de períodos de retenção diferentes para arquivos individuais, armazenados através dos protocolos CIFS e/ou NFS. Esta funcionalidade deverá ser licenciada sem limite de capacidade do sistema, mesmo no crescimento de área de dados até o limite máximo do sistema;
- Deverá integrar com servidor antivírus externo, conectados via rede ao Sistema de Armazenamento de Dados. A funcionalidade deve permitir selecionar os tipos de arquivos que devem ser verificados pelo servidor de antivírus. Se for detectado que o arquivo está infectado, a funcionalidade deve permitir a configuração de uma limpeza automática. Deverá suportar os seguintes fornecedores de software de antivírus: Symantec, Norton, McAfee, CA, TrendMicro e Sophos.
- Deverá ser RoHS Compliance, ou seja, com restrição ao uso de certas substâncias perigosas no processo de fabricação de produtos, como Chumbo (Pb), Cádmio (Cd), Mercúrio (Hg), Cromo hexavalente (Hex-Cr), bifenilos polibromados (PBBs) e éteres difenil-polibromados (PBDEs);
- Possuir ferramenta de gerência do sistema com interface gráfica em web, com acesso seguro https/ssl, incluindo a geração de gráficos de desempenho através da interface web. Caso isso não seja possível deverão ser fornecidos todos os recursos de software e hardware necessários para o gerenciamento e a monitoração do sistema;
- Disponibilizar interface de linha de comando com acesso seguro ssh (in-band) e através de conexão por cabo direto na controladora;
- Possuir mecanismo de monitoramento de todo o sistema em tempo real;
- Possuir sistema de monitoramento remoto por central de suporte do fabricante;
- Gerar alertas, logs e notificações de eventos críticos e falhas;
- Permitir controle de acesso à interface de gerenciamento mediante autenticação no Microsoft Active Directory;
- Suportar pelo menos “leitura e escrita” e “somente leitura” como perfis de acesso para atribuição a usuários;

- Disponibilizar, por meio da interface gráfica, dados históricos e informações que permitam monitoramento de recursos, identificação de problemas e avaliações de desempenho;
- Gerar alertas, logs e notificações de eventos críticos e falhas;
- Disponibilizar plugin para o VMware vCenter versão 4.1 e superiores;
- Ser totalmente compatível com o cluster de controladoras especificado.
- Permitir monitoramento por meio do protocolo SNMP;
- Todas as funcionalidades acima e licenciamentos solicitados deverão ser fornecidas licenciadas para a capacidade máxima de armazenamento do subsistema de armazenamento ofertado.

9.7. Deverá ser entregue, também, com uma capacidade líquida mínima de armazenamento de 10UTB (Dez Tera Bytes úteis) sendo:

- Área calculada em base 2, isto é, 1 TB (terabyte) é igual a 1.099.511.627.776 bytes;
- Área líquida deve excluir toda e qualquer área destinada para outra finalidade que não seja armazenamento de dados dos sistemas e dos usuários, como por exemplo, formatação, “right sizing”, controle e/ou pools de discos destinados ao sistema operacional do sistema de armazenamento, e outros que por ventura façam parte da implementação da solução ofertada;
- Área líquida não pode incluir discos de hot-spare;
- Área líquida não pode incluir discos de espelhamento e/ou paridade relativos ao RAID solicitado;

9.8. Deverá ser fornecido e configurado com discos do tipo SAS de velocidade mínima de 15krmp.

9.9. Deverá ser fornecido e implantado com proteção física de discos através da tecnologia RAID, que garanta a integridade e a disponibilidade dos dados, mesmo no caso de falha de até quaisquer 2 discos de dados no mesmo raid group.

9.10. Deverá possuir no mínimo 2 controladoras ativas, não sendo aceitas soluções de agregação como Cluster para atendimento das quantidades de portas e cache.

9.11. Deverá ser fornecido com, no mínimo, 4 portas FC de 8 Gbps por controladora, com conectores LC para conexões aos servidores ou FC switches / directors.

9.12. Deverá ser fornecido com, no mínimo, 4 portas de 1 Gbps Ethernet TP por controladora, para conexão dos sistemas computacionais dos clientes.

9.13. Deverá ser fornecido com, no mínimo, 2 portas de 10 Gbps Ethernet TP por controladora, para conexão dos sistemas computacionais dos clientes; permitindo a utilização simultânea e segmentada da conexão pelos protocolos iSCSI, FCoE, CIFS e NFS.

9.14. Deverá ser fornecido com, no mínimo, 6 GB de capacidade de memória cache por controladora, tendo o sistema completo a quantidade mínima de 12 GB de cache.

10. Switch gigabit e conexão com redes externas:

10.1. Os switches existentes e a estrutura de rede atual serão desativados e substituídos pelos equipamentos descritos a seguir.

10.2. **Chassis Básico:**

10.2.1. Os equipamentos que compõem a solução deverão possuir, individualmente, no máximo 2 Rack Unit (RU) – 3,5''.

10.2.2. Os equipamentos deverão ser montáveis em rack de 19'', devendo vir acompanhados dos devidos acessórios para tal.

10.2.3. Os equipamentos deverão ser de primeira qualidade, novos, sem uso, de fabricação recente (fabricado no máximo a 6 meses antes da data de entrega) e com acabamento apropriado.

10.3. **Desempenho**

10.3.1. Os equipamentos devem possuir hardware específico com tecnologia ASICs (Application-Specific Integrated Circuits) para tratar (filtros, policies, etc.) frames Layer 2 (Ethernet).

10.3.2. A capacidade de Switch Fabric da solução deve ser de no mínimo 176Gbps.

10.3.3. A capacidade de processamento da solução deve ser de no mínimo 130Mpps.

10.4. **Memória**

10.4.1. Deve possuir Memória Flash com capacidade de armazenamento mínima de 2 vezes o tamanho da imagem do Sistema Operacional a ser entregue.

10.4.2. Realizar o upload e download da configuração.

10.5. **Fonte de alimentação**

10.5.1. Deve possuir fonte de alimentação de energia elétrica com chaveamento automático entre 100/240V AC.

10.5.2. A fonte de alimentação instalada deverá ser interna ao chassis.

10.5.3. A fonte de alimentação instalada deverá ser do tipo “hot-insertable” e “hot-removable”.

10.5.4. A fonte de alimentação instalada deverá alimentar e suportar a configuração solicitada.

10.5.5. Deve possuir uma segunda fonte de alimentação de energia elétrica, interna, com chaveamento automático entre 100/240V AC.

10.5.6. A fonte de alimentação redundante deve ser interna ao chassis, não necessitando de equipamento ou fonte externa.

10.5.7. Em caso de falha de fonte principal a redundante deverá alimentar e suportar sozinha a configuração solicitada, e vice-versa.

10.5.8. Deve possuir módulo de fans, o qual pode ser trocado independentemente da fonte de alimentação.

10.6. **Portas**

10.6.1. Todas as portas devem implementar o padrão IEEE 802.3ad – Link Aggregation.

10.6.2. Quantidade mínima de LAGs (Links Aggregation) suportados: 32.

10.6.3. Algoritmo de balanceamento de carga em LAGs:

- IP: S/D MAC, S/D IP
- TCP/UDP: S/D MAC, S/D IP, S/D Port
- Non-IP: S/D MAC

10.6.4. Quantidade mínima de portas suportadas por LAG: 8.

10.6.5. Todas as portas devem implementar a configuração estática e dinâmica via LACP (Link Aggregation Control Protocol).

10.6.6. Devem implementar o trunking groups com 8 (oito) portas ativas ou mais.

10.6.7. Todas as portas devem implementar o Jumbo Frame com tamanho mínimo de 9KB.

10.6.8. Deve possuir no mínimo 4 portas ópticas de 10GB para 40km.

10.6.9. Deve possuir no mínimo 48 portas RJ-45 10/100/1000BASE-Tx.

10.7. **Portas 10 Gigabit Ópticas**

10.7.1. Devem possuir um mínimo de 4 (quatro) portas 10GBase-X (10 Gigabit) de uplink populadas com as interfaces com as quais devem garantir conexão de 40Gbps até o Switch de Core.

10.7.2. As portas devem ser compatíveis com o padrão IEEE 802.3ae.

10.7.3. As portas 10 GBase-X devem ser do tipo SFP+ (10 Gigabit Small Form-factor Pluggable) ou XFP e devem ser hot-swappable.

10.7.4. Caso as portas 10GBase-X sejam do tipo XFP, estas deverão ser fornecidas com seus respectivos módulos XFP do tipo Short Reach.

10.7.5. Caso as portas sejam do tipo SFP+, estas deverão suportar cabos do tipo Direct-Attached Copper Cable, ou seja, interfaces conectorizadas baseadas em cabos de cobre twinax que possibilitam a interconexão em 10Gbps.

10.7.6. As portas, independentemente da tecnologia, deverão ser fornecidas com a respectiva interface Short Reach

10.7.7. Deverão acompanhar 1 par do cabo do tipo Direct-Attached Copper Cable, ou seja, interfaces conectorizadas baseadas em cabos de cobre twinax que possibilitam a interconexão em 10Gbps com o switch tipo 3.

10.8. **Expansão de Portas**

10.8.1. A solução proposta deve permitir agrupamento de equipamentos semelhantes sob uma das formas a seguir (independentemente da terminologia utilizada pelo fabricante):

a) Empilhamento (Stacking) OU
b) Chassi Virtual.

10.8.2. Empilhamento é entendido como a interligação de equipamentos (no mínimo 8) compondo uma pilha ou cluster. Sob o ponto de vista da gerência os equipamentos se comportam como um único switch. Em caso de falha de um deles, qualquer outro equipamento assume a condição de master, garantindo proteção 1:N.

10.8.3. Chassi virtual é entendido como a composição de elementos, sendo um deles supervisor e os demais conectados a ele. Os elementos conectados ao elemento supervisor se comportam como módulos de expansão deste, possuindo todas suas funcionalidades. Cada chassi virtual deve comportar no mínimo 256 portas de acesso. Para cada 8 módulos do chassi virtual deverá ser fornecido um elemento supervisor.

10.8.4. No caso de fornecimento de equipamento em sites distintos, não serão aceitos módulos sem elemento supervisor.

10.8.5. A pilha ou chassi virtual deve se comportar como um switch único, em termos de gerenciamento, além de possibilitar Link Aggregation (IEEE 802.3ad) entre qualquer conjunto de portas do agrupamento, independemente do chassi físico em que elas se localizam. Da mesma forma deve ser possível a aplicação de Mirroring entre portas de chassis físicos diferentes, desde que os mesmos façam parte do mesmo agrupamento.

10.8.6. Caso seja implementado Empilhamento, o equipamento deverá possuir adicionalmente portas dedicadas para tal, as quais totalizarão um mínimo de 40 Gbps (20 Gbps Full Duplex).

10.8.7. O empilhamento não pode utilizar as 2 portas 10 Gigabit ópticas utilizadas para uplink.

10.8.8. Deverão ser fornecidos os cabos, módulos e interfaces ópticas (por exemplo, XFP ou SFP+), quando necessários, para que o empilhamento ou chassi virtual possa ser implementado.

10.9. **Switching (L2)**

10.9.1. Capacidade mínima da tabela de endereçamento MAC por módulo, pilha ou chassi virtual: 24k.

10.9.2. Deve implementar o switching em camada 2.

10.9.3. Deve implementar o padrão IEEE 802.3x – Flow Control.

10.9.4. Deve implementar o padrão IEEE 802.1Q – VLAN ID Tagging.

10.9.5. Capacidade mínima de VLANs por pilha ou chassi virtual (não considerar mecanismos multiplicadores como por exemplo Q-in-Q): 4090.

10.9.6. Permitir a utilização simultânea de todas as VLANs.

10.9.7. Deve implementar VLANs baseada em: Port-Based.

10.9.8. Deve implementar o padrão IEEE 802.1D – Classic Spanning Tree

10.9.9. Deve implementar o Spanning Tree por VLAN com no mínimo 16 (dezesseis) domínios de Spanning Tree.

10.9.10. Deve implementar o padrão IEEE 802.1w – Rapid Spanning Tree.

10.9.11. Deve implementar o padrão IEEE 802.1s – Multiple Spanning Tree.

10.9.12. Deve implementar a limitação da quantidade de endereços MAC por porta.

10.9.13. Deve implementar mecanismos de proteção contra pacotes BPDU (bridge protocol data unit) recebidos em uma porta de acesso.

10.9.14. Deve implementar o Aging L2 Global ou por VLAN. O equipamento exclui os L2 MAC address não utilizados na tabela de entrada Porta/MAC Address.

10.9.15. Deve implementar no mínimo 256 grupos de Multicast por pilha ou chassi virtual.

10.9.16. Deve implementar totalmente o IGMP v1 e v2.

10.10. **Switching (L3)**

10.10.1. Deve implementar o roteamento IPv4 entre as VLANs configuradas no equipamento.

10.10.2. Deve implementar o roteamento IPv4 estático.

10.10.3. Deve implementar os protocolos de roteamento RIPv1 (RFC1058), RIPv2 (RFC1723 ou RFC2453).

10.10.4. Deve implementar o protocolo de roteamento OSPFv2 (RFC2178 ou RFC2328).

10.10.5. Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol) (RFC3768 ou RFC2338).

10.10.6. Capacidade mínima de rotas IPv4 unicast: 8K.

10.10.7. Capacidade mínima de rotas IPv4 multcast: 2K.

10.10.8. Deve implementar no mínimo 256 grupos de Multicast por pilha ou chassi virtual.

10.10.9. Deve implementar PIM-SM (RFC4601 e RFC5059 ou RFC2362 ou Draft IETF PIM-SM-v2).

10.10.10. Quando o fabricante implementar funcionalidades de IPv6, estas funcionalidades deverão ser fornecidas sem custo.

10.11. **COS e QOS - Classes De Serviço E Qualidade De Serviço**

10.11.1. Deve implementar a classificação e priorização de pacotes de acordo com os seguintes campos:

- Campo PCP Priority Code Point (IEEE 802.1p).
- Campo IP Precedence/ToS do cabeçalho IPv4 (quando fornecidas funcionalidades L3).
- Campo DSCP/ToS do cabeçalho IPv4 (quando fornecidas funcionalidades L3).
- Endereço IP Origem (quando fornecidas funcionalidades L3).
- Endereço IP Destino (quando fornecidas funcionalidades L3).
- Port TCP/UDP de origem.
- Port TCP/UDP de destino.
- Interface de entrada (física).
- Endereço MAC.

10.11.2. De acordo com a classificação local o equipamento define as filas de saída associadas a cada pacote.

10.11.3. Deve suportar reescrita dos campos PCP/IEEE 802.1p e DSCP quando o pacote sai do equipamento.

10.11.4. Deve possuir um mínimo de 8 (oito) filas de prioridade (QoS) por porta.

10.11.5. Deve implementar os algoritmos de queue scheduling Weighted Round Robin e Strict Priority Queue.

10.12. **Gerenciamento**

10.12.1. Deve possuir uma interface ethernet RJ-45 autosense (10/100 Mbps) para gerenciamento “out-of-band”.

10.12.2. Deve possuir uma interface RS-232 ou RJ-45 para conexão a equipamento console (emulador de terminal assíncrono tipo VT-100).

10.12.3. Deve implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento.

10.12.4. Deve implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol).

10.12.5. Deve implementar o padrão IEEE 802.1ab - The Link Layer Discovery Protocol (LLDP) ou Cisco Discovery Protocol (CDP).

10.12.6. Deverá fornecer o software de gerenciamento dos equipamentos propostos, com todas as funcionalidades e licenças disponíveis para no mínimo 40 equipamentos, sem custos adicionais.

10.12.7. Esta é uma ferramenta que permite configurar, monitorar, gerenciar, inventariar e realizar troubleshooting na rede composta pelos equipamentos e seus elementos de forma centralizada a partir de um servidor.

10.13. **Configuração**

10.13.1. Deve permitir acesso in-band via TELNET e SSHv2.

10.13.2. Deve permitir o FTP ou TFTP como mecanismo de transferência de arquivos de configuração e Sistema Operacional.

10.14. **CLI - Command Line Interface**

10.14.1. Deve possuir auto-complementação de comandos.

10.14.2. Deve possuir ajuda contextual.

10.14.3. Deve permitir Autenticação e Autorização local, e através de servidor específico com protocolo RADIUS.

10.14.4. Deve permitir vários níveis de privilégio de acesso a usuários.

10.14.5. Deve possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps, ou valor percentual).

10.15. **SNMP**

10.15.1. Deve possuir total compatibilidade com os protocolos de gerenciamento SNMPv1, SNMPv2 (RFC1257) e SNMPv3.

10.15.2. Deve possuir total compatibilidade com o protocolo RMON.

10.15.3. Deve implementar o RMON, para mínimo de 4 (quatro) grupos.

10.15.4. Deve possuir total compatibilidade com traps SNMP conforme definido na RFC 1215.

10.15.5. Deve possuir MIBs compiláveis na plataforma HP Open View Network Node Manager.

10.15.6. Deve fornecer todas as MIBs do equipamento sem nenhum custo adicional.

10.16. **Syslog**

10.16.1. Deve possuir geração de mensagens de syslog para eventos relevantes ao sistema.

10.16.2. Deve possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog.

10.16.3. Deve possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento.

10.17. **Segurança**

10.17.1. Deve implementar filtros (ACL – Access List) de pacotes em qualquer interface física e lógica. As ACLs deverão ser implementadas de forma que não prejudique a CPU do equipamento.

10.17.2. Deve implementar regras de filtros (ACL – Access List) considerando qualquer combinação dos seguintes parâmetros:

- Endereço IPv4 de origem (quando fornecidas funcionalidades L3).
- Endereço IPv4 de destino (quando fornecidas funcionalidades L3).
- Endereço MAC de origem.
- Endereço MAC de destino.
- Protocolo.
- Port TCP/UDP de origem.
- Port TCP/UDP de destino.
- Tipo ICMP.

10.17.3. Quantidade de filtros (ACL – Access List) simultâneos possíveis de serem implementados por chassi virtual, módulo ou pilha: 1K.

10.17.4. Deve implementar filtros para controle de acesso SNMP, TELNET e SSHv2.

10.17.5. Deve registrar em um log as tentativas de violação de filtros de pacotes em um Syslog Server.

10.17.6. Deve implementar mecanismos automáticos de proteção contra ataques de Denial of Service (DoS) com bloqueio do tráfego na entrada da interface.

10.17.7. Deve implementar mecanismos automáticos de proteção aos protocolos L2 e L3 (quando suportado) contra ataques de rede com limitação de banda para tráfegos de broadcast-storm e multicast.

10.18. **Troubleshooting**

10.18.1. Deve possuir ferramentas básicas de diagnóstico de rede (telnet, traceroute e ping).

10.18.2. Deve implementar o Port Mirroring.

10.18.3. Deve implementar Debugging: CLI via console, telnet ou SSH.

10.18.4. Deve armazenar um log de eventos no próprio equipamento ou chassi virtual para consulta via command line (CLI).

10.19. **Sistema Operacional**

10.19.1. Deve implementar o FTP ou TFTP como mecanismo de transferência de arquivos para atualizações do sistema operacional.

10.20. **Certificado de Homologação da Anatel**

10.20.1. O proponente deverá apresentar o certificado de homologação da ANATEL do equipamento proposto até a data de entrega desses equipamentos, sob pena de recusa.

10.21. **Condições Gerais de Fornecimento**

10.21.1. Os equipamentos deverão ser embalados individualmente, com embalagem apropriada que garanta proteção durante o transporte.

10.21.2. Todo o processo de instalação deverá ser realizado pelo proponente.