ESPECIFICAÇÕES TÉCNICAS

ITEM 1 - SWITCH DE NÚCLEO

1.1. Switch para a utilização de módulos de interfaces de I/O;
1.2. A comunicação entre cada módulo de interface e o backplane deve ser de, no mínimo, 40 Gbps;
1.3. Deve possuir módulos de supervisão/gerência, controle e switch fabric redundantes. Entende-se por módulo de supervisão/gerência o ativo indispensável ao funcionamento do switch que, além de gerenciar o chassi, provê a comutação em todo o equipamento, encaminhando o tráfego entre portas de diferentes módulos de interface;
A) Caso a solução implemente redundância distribuída ou full mesh é entendido como redundância nativa;
1.4. Deve possuir performance mínima de 160Gbps e 200 Mpps;
1.5. Deve suportar sincronismo entre informações de nível 2 e 3 contidas nos processadores e supervisores, de modo que na perda de um processador ou supervisor primário não ocorra reconvergência;
A) Caso a solução seja distribuída ou full mesh é entendido como redundância nativa da arquitetura;
1.6. Para a solução centralizada (switch fabric):
A) Todos os módulos de interfaces instalados deverão implementar comutação distribuída do tipo DFC (Distributed Forwarding Card) ou similar entre os módulos do switch, ou seja, o tráfego entre portas do mesmo módulo não deve ser encaminhado para o módulo de gerência/processamento, tanto no nível dois quanto no nível três da camada OSI. É permitido apenas que os primeiros pacotes do fluxo vão até o switch fabric para estabelecimento do fast-path no módulo;
1.7. Para a solução Distribuída ou Full Mesh:
A) Caso a solução seja distribuída ou full mesh é entendido como comutação distribuída nativa da arquitetura;
1.8. Possuir fontes redundantes para as configurações (inicial e futura) solicitadas. As fontes deverão ser fornecidas na quantidade N+1, sendo N a quantidade necessária ao pleno funcionamento do equipamento em sua capacidade máxima;
1.9. As fontes de alimentação devem ser hot-swap e dispor de sistema de Load Sharing;
1.10. Fontes de alimentação para operação em rede elétrica 110/220V – 60Hz, com seleção automática de tensão;
1.11. Possuir tabela MAC com, no mínimo, 32.000 (trinta e duas mil) entradas;
1.12. O Equipamento deve suportar:
A) A instalação de até 24 portas 10 Gigabit Ethernet 10GBase-X com conectores SC ou LC;
1.13. Todos os componentes que tem comunicação direta com o backplane (módulos de supervisão/gerencia (caso possua), fontes de alimentação, fans e módulos de interface) devem ser hot-swap e permitir a sua instalação/remoção pela parte frontal do chassi;
1.14. Deverá operar em temperaturas que possam variar entre 10º a 40º C, com umidade relativa do ar variando até 90% não condensante;
1.15. Deve implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9.000bytes;
1.16. Deverá ser fornecido cabo console, cabos de alimentação elétrica necessários para o funcionamento do equipamento e manuais de operação e instalação;

Gerenciamento

1.17. Gerenciamento do chassi através de um único endereço IP;
1.18. Possuir porta de console, tipo RS-232 ou RJ-45;
1.19. Deve Implementar Secure Shell (SSHv2) e Telnet;
1.20. Deve implementar SNMPv2c e SNMPv3, com autenticação e/ou criptografia;
1.21. Deve possuir CLI (Command Line Interface);
1.22. Deve possuir software de gerenciamento gráfico através de servidor web interno, garantindo o acesso através de um web browser comum ou outro mecanismo similar;
1.23. Deve possuir FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol);
1.24. Deve permitir tratamento do tráfego de protocolos para a gerência da rede;
1.25. Deve suportar as MIBs I e II;
1.26. Deve suportar NetFlow v5 ou superior ou SFlow;
1.27. Deve suportar syslog;
1.28. Deve suportar múltiplas imagens do sistema operacional;
1.29. Deve suportar múltiplas imagens de arquivo de configuração;
1.30. Permitir o download e o upload das configurações;
1.31. Deve implementar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
1.32. Deve suportar proteção contra-ataques DoS ou DDoS destinados a sobrecarregar a CPU do equipamento ou realizar controle de broadcast storm;

1.33. Deve possuir facilidade que permita desabilitar automaticamente uma interface de acesso que esteja recebendo pacotes BPDU (Bridge Protocol Data Unit);
1.34. Deve implementar o protocolo CDP ou funcionalidade para descobrimento automático da topologia da rede com o fornecimento de informações de configurações da Camada 2 de todos os dispositivos conectados, de acordo com o padrão 802.1ab (LLDP);
1.35. Deve ser possível espelhar o tráfego de portas que residem em um dado módulo para uma porta que reside em outro módulo do mesmo switch;

a) Deve implementar espelhamento de tráfego Inbound e Outbound, inclusive entre portas de módulos distintos;

1.36. Deve implementar espelhamento de tráfego de forma que o tráfego de várias portas possa ser espelhado em outra para fins de monitoramento e diagnósticos. Deve permitir no mínimo 2 (duas) sessões de espelhamento simultâneas por chassi;
1.37. O equipamento deverá ser entregue com os módulos e licenças de gerenciamento do equipamento e dos demais módulos fornecidos.

Funções de Camada 3 e 2 (L3 e L2)

1.38. Deve implementar Link Aggregation – 802.3ad entre módulos de interfaces diferentes;
1.39. Deve implementar no mínimo 40 grupos de agregação 802.3ad, sendo que cada grupo deve ter pelo menos 8 (oito) portas independentes do tipo da porta (par trançado ou fibra) e velocidade (Gigabit Ethernet ou 10 Gigabit Ethernet) juntos no mesmo grupo;
1.40. Deve implementar o protocolo GVRP ou VTP ou similar em funcionalidades;
1.41. Deve suportar IPv6 para gerenciamento;
1.42. Deve implementar Layer 3 switching, roteamento IPV4 estático;
1.43. Deve implementar roteamento dinâmico OSPFv2 e Policy-based Routing e RIP e RIPv2;
1.44. Deve implementar IGMP v1 e v2 e snooping;
1.45. Deve implementar IP Multicast Routing (PIM-SM ou PIM-DM), MSDP ou DVMRP;
1.46. Deve implementar DHCP Relay e/ou Server;
1.47. Deve implementar ECMP (Equal cost Multi-Path) com 8 (oito) caminhos simultâneos, pelo menos;
1.48. Deve implementar um mínimo de 15.000 rotas;
1.49. Deve implementar IEEE 802.1q, Spanning Tree – 802.1d/802.1w/802.1;
1.50. Deve implementar no mínimo 4.000 VLAN's simultâneamente;
1.51. Deve implementar o protocolo VRRP ou HSRP;
1.52. Deve suportar no mínimo 256 interfaces de VRRP ou HSRP;

QoS

1.53. Quality of Service (QoS), classificação, marcação de pacotes e priorização de tráfego baseada nos padrões IEEE 802.1p (CoS) e Diffserv (DSCP), "Traffic Policing" e "Traffic Shaping";
1.54. Deve implementar o gerenciamento de banda de entrada (rate limit), sendo que a banda mínima deve ser de 512 KBps (KiloBytes por segundo);
1.55. Deve implementar o controle de banda de saída (rate shapping), sendo que a banda mínima deve ser de 512 KBps (kiloBytes por segundo);
1.56. Pelo menos 8 (oito) filas por porta, em hardware, para tratamento de QoS;
1.57. Implementar classificação de tráfego baseada no endereço MAC de origem e destino, IP de origem e destino e portas TCP e UDP de origem e destino;
1.58. Deve implementar os algoritmos de enfileiramento Strict Priority e/ou Round-Robin com ponderação (Weighted Fair Queue, weighted Round Robin ou Shaped Round Robin);

Segurança

1.59. Deve implementar autenticação via Tacacs+ e Radius;
1.60. Deve implementar o padrão IEEE 802.1x (network login), permitindo configuração automática da VLAN e aplicação de ACL ou policy sendo que estes parâmetros devem ser aplicados de acordo com o perfil de cada usuário;
1.61. Implementar no mínimo 2 (dois) usuários autenticados na mesma porta de acordo com o IEEE 802.1x, sendo que os perfis de regras de controle de acesso, VLAN's e QoS devem ser diferentes para cada usuário;
1.62. Implementar listas de controle de acesso ou funcionalidade similar de controle para restringir o acesso ao serviço telnet e SSH do switch;

1.63. Deve ser possível configurar explicitamente os endereços MACs que podem ser aprendidos em uma porta do switch;
1.64. Deve ser possível informar, por porta do switch, a quantidade de endereços MACs que podem ser aprendidos dinamicamente, devendo permitir a configuração do valor mínimo para 01 (um) endereço MAC;
1.65. Deve permitir envio de trap SNMP quando ocorrer uma violação de filtro de MAC das situações acima;

Geral

1.66. Deverá ser apresentado o certificado de homologação na ANATEL, conforme resolução 242. O certificado deve estar emitido especificamente para a marca e modelo do produto ofertado e o mesmo deve estar disponível no sitio da Anatel para consulta;
1.67. A Licitante deverá apresentar garantias de que os produtos ofertados são de origem comprovada e que possuem garantia do fabricante no território nacional, independente da garantia ofertada pela própria Licitante;
1.68. A Licitante deverá comprovar que possui autorização para comercialização, instalação e suporte dos equipamentos ofertados. A comprovação poderá ser feita através de declaração do fabricante.

ITEM 2 - INTERFACE 10 GIGABI ETHERNET – SR

2.1. Deve ser compatível com os switches de Core e do mesmo fabricante;
2.2. Transceiver óptico padrão 10 Gigabit padrão 10GBase-SR para fibra óptica multimodo
2.3. Padrão SFP+ com conector LC
2.5. Deve ser totalmente compatível com todos os switches aqui descritos, sendo que todos os acessórios do fabricante necessários à instalação no equipamento descrito no referido item deverão ser entregues;
2.6. Deve acompanhar cordão óptico duplex com comprimento mínimo de 2,5 metros com conectores LC/LC. O cordão pode ser de outro fabricante da interface.

ITEM 3 - INTERFACE 1 GIGABIT ETHERNET BaseT

3.1. Deve ser compatível com os switches de Core e do mesmo fabricante;
3.3.2. SFP 1 Gigabit padrão 1000Base-T para cabo RJ-45;
3.3.3. Deve ser totalmente compatível com todos os switches aqui descritos, sendo que todos os acessórios do fabricante necessários à instalação no equipamento descrito no referido item deverão ser entregues;

ITEM 4 - SWITCH DE ACESSO TIPO I

4.1. Deve ser instalado em rack padrão EIA (19”) e possuir kits completos para instalação;
4.2. Deve possuir altura máxima de 1 Ru;
4.3. Deve possuir, no mínimo, 48 (quarenta e oito) portas 10/100/1000 Base T diretamente conectada ao chassi;
4.4. Deve possuir, no mínimo, 02 (dois) slots/portas do tipo SFP, fixas ao equipamento, para instalação de portas os padrões 1000BaseSx,1000BaseLx e 1000BaseT em qualquer combinação;
4.5. Deve possuir, no mínimo, 02 (dois) slots/portas do tipo SFP+ ou XFP, fixo ao equipamento, para a instalação de portas nos padrões 10 GBase-SR, 10Gbase-LRM e 10 Gbase-LR;
4.6. Deve possuir 02 (duas) portas nativas ao equipamento e fixas ao chassi e ainda específicas para empilhamento (stack), com desempenho mínimo de 24 (Vinte e Quatro) Gbps por porta. Não será aceito equipamento que se utilize de recurso de agregação para atingir a performance solicitada por porta. Não será aceito produto com tecnologia de empilhamento por cluster ou que utilize de interfaces RJ45 ou SFP ou SFP+ ou X2 ou XENPACK ou CX4 para realizar o empilhamento;
4.7. Deve permitir o uso simultâneo de, no mínimo, 48 (quarenta e oito) portas Gigabit Ethernet, 2(duas) portas 10Gigabit Ethernet e 2 (duas) portas dedicadas a função de empilhamento;
4.8. Deve possuir porta console RS-232 com conectores DB9 ou RJ-45;
4.9. Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 110 e 220 VAC e suporte frequência entre 50/60hz;
4.10. Deve implementar alimentação elétrica pelo cabo ethernet de acordo com os padrões:
    A) IEEE 802.3at;
    B) IEEE 802.3af;
4.11. Deve possuir fonte de alimentação com potência mínima de 370 watts para alimentação de dispositivos POE;
4.12. Deve possuir capacidade de habilitar/desabilitar o POE por porta;

4.13. Deve possuir mecanismos de proteção contra sobrecarga e/ou curto-circuito no POE;
4.14. Deve suportar fonte redundante externa;

Capacidade
4.15. Deve Implementar no mínimo 130 Mpps;
4.16. Deve Implementar switch fabric de no mínimo 136 Gbps, ou seja, wirespeed;
4.17. Deve Implementar tabela de endereçamento para, no mínimo, 16.000 (doze mil) endereços MAC;
4.18. Deve Implementar no mínimo 512 (quinhentos e doze) VLANs ativas - IEEE 802.1Q;

Protocolos
4.19. Deve Implementar IEEE 802.1Q;
4.20. Deve Implementar IEEE 802.1s;3
4.21. Deve Implementar IEEE 802.3x;
4.22. Deve Implementar IEEE 802.1D;
4.23. Deve Implementar IEEE 802.1w;
4.24. Deve Implementar IEEE 802.3ad, 06 (seis) LAGs com 08 (oito) portas por LAG, inclusive entre portas de switches distintos da pilha;
4.25. Deve Implementar IGMP v1 e v2 e snooping;
4.26. Deve Implementar Broadcast Suppression por porta;
4.27. Deve Implementar Jumbo Frame 9000 bytes;
4.28. Deve Implementar o padrão IEEE 802.1ab e LLDP-MED;

Empilhamento
4.29. Deve permitir empilhar, no mínimo, 8 (oito) unidades;
4.30. Deve permitir o gerenciamento do switch e da pilha de switches através de endereço IP único;
4.31. Deve possuir 02 (duas) portas fixas ao chassi e específicas para empilhamento (stack), com desempenho mínimo de 10 (dez) Gbps por porta;
4.32. Deve suportar empilhamento redundante, através da ligação do último switch da pilha ao primeiro switch da pilha;
4.33. Deve permitir o empilhamento com o switch de acesso tipo II;

Roteamento
4.34. Deve implementar roteamento IP no mínimo para:
4.35. Rota estática;
4.36. RIP v1;
4.37. RIP v2;
4.38. Deve suportar no mínimo 60 (sessenta) rotas estáticas;
4.39. Deve suportar no mínimo 255 (duzentos e cinquenta e cinco) rotas RIP;
4.40. Deve implementar DHCP Relay;

Qualidade de serviço
4.41. Deve implementar IEEE 802.1p;
4.42. Deve implementar Rate Limiting por porta;
4.43. Deve realizar classificação de tráfego: por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS;
4.44. Deve possuir a capacidade de associar um dispositivo autenticado por 802.1x a uma respectiva VLAN e ainda associar este dispositivo a política de filtragem de tráfego e de qualidade de serviço;
4.45. Deve possuir a capacidade de associar um dispositivo autenticado por endereço MAC a uma respectiva VLAN e ainda associar este dispositivo a política de filtragem de tráfego e de qualidade de serviço;
4.46. Deve implementar a remarcação do campo ToS (Type of Service);
4.47. Deve possuir no mínimo 6 (seis) filas de prioridade por porta;
4.48. Deve possuir algoritmo de enfileiramento Strict Priority e Weighted Round Robin;

Segurança
4.49. Deve permitir o controle de acesso a rede baseado no endereço MAC;

4.50. Deve ser possível configurar explicitamente os endereços MACs que podem ser aprendidos em uma porta do switch;
4.51. Deve ser possível informar, por porta do switch, a quantidade de endereços MACs que podem ser aprendidos dinamicamente, devendo permitir a configuração do valor mínimo para 1 (um) endereço MAC;
4.52. Deve implementar envio de trap SNMP quando ocorrer uma violação de filtro de MAC das situações acima;
4.53. Deve implementar IEEE 802.1X Port-Based Network Access Control de acordo com a RFC 3580;
4.54. Deve suportar autenticação via web para usuários visitantes, podendo a login ser feito na base local do switch ou através de Radius;
4.55. Deve suportar no mínimo 3 autenticações por porta;
4.56. Deve implementar autenticação de dispositivos através de endereço MAC, realizando a validação do endereço MAC em servidor Radius;
4.57. Deve implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS;
4.58. Deve implementar broadcast suppression por porta;
4.59. Deve implementar recurso para possibilitar que uma interface executando o protocolo Spanning Tree seja colocada no estado down quando a mesma receber um BPDU;
4.60. Deve implementar funcionalidade que bloqueie a operação de servidores DHCP inválidos (DHCP Spoof);
4.61. Deve implementar funcionalidade de Arp Spoof protection;
4.62. Deve implementar recurso de private VLAN ou protected port;

Gerenciamento

4.63. Deve implementar SSH V2;
4.64. Deve implementar SNMP v1, v2c e v3;
4.65. Deve suportar IPv6 para gerenciamento;
4.66. Deve implementar NTP ou SNTP;
4.67. Deve implementar Syslog Permitindo configurar no mínimo 02 (dois) servidores de syslog distintos;
4.68. Deve implementar Radius e TACACS+;
4.69. Deve implementar mecanismo interno ao switch de teste de cabo metálico RJ-45 sendo possível obter, no mínimo, as seguintes informações:
4.70. Status operacional do cabo (ativo ou falha);
4.71. Tamanho aproximado do cabo;
4.72. Status de crosstalk ou falha de pinagem;
4.73. Deve implementar espelhamento de tráfego, inclusive entre portas de switches distintos da pilha. Deve permitir espelhar simultaneamente os frames recebidos e transmitidos;
4.74. Deve implementar Telnet;
4.75. Deve implementar TFTP ou FTP;
4.76. Deve Implementar CLI;
4.77. Deve implementar Sflow ou Netflow v5 ou Netflow v9;
4.78. Deve implementar RMON, 04 (quatro) grupos, sem utilização de probe externa;
4.79. Deve implementar gerenciamento por HTTP ou HTTPS através de acesso direto ao equipamento por web browser padrão;
4.80. Deve suportar, no mínimo, 02 (duas) Imagens do sistema operacional e 2 (dois) arquivos de configuração.

ITEM 5 - SWITCH DE ACESSO TIPO II

5.1. Deve ser instalado em rack padrão EIA (19") e possuir kits completos para instalação;
5.2. Deve possuir altura máxima de 1 Ru;
5.3. Deve possuir, no mínimo, 24 (vinte e quatro) portas 10/100/1000 Base T diretamente conectada ao chassi;
5.4. Deve possuir, no mínimo, 02 (dois) slots/portas do tipo SFP+ ou XFP, fixo ao equipamento, para a instalação de portas nos padrões 10 GBase-SR, 10Gbase-LRM e 10 Gbase-LR;
5.5. Deve possuir 02 (duas) portas específicas para empilhamento (stack), com desempenho mínimo de 24 (Vinte e Quatro) Gbps por porta. Não será aceito equipamento que se utilize de recurso de agregação para atingir a performance solicitada por porta. Não será aceito produto com tecnologia de empilhamento por cluster ou que utilize de interfaces RJ45 ou SFP ou SFP+ ou X2 ou XENPACK ou CX4 para realizar o empilhamento;
5.6. Deve permitir o uso simultâneo de, no mínimo, 24 (vinte e quatro) portas Gigabit Ethernet, 2(duas) portas 10Gigabit Ethernet e 2 (duas) portas dedicadas a função de empilhamento;
5.7. Deve possuir porta console RS-232 com conectores DB9 ou RJ-45;

5.8. Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 110 e 220 VAC e suporte frequência entre 50/60hz;
5.9. Deve implementar alimentação elétrica pelo cabo ethernet de acordo com os padrões:
5.10. IEEE 802.3at;
5.11. IEEE 802.3af;
5.12. Deve possuir fonte de alimentação com potência mínima de 370 watts para alimentação de dispositivos POE;
5.13. Deve possuir capacidade de habilitar/desabilitar o POE por porta;
5.14. Deve possuir mecanismos de proteção contra sobrecarga e curto-circuito no POE;
5.15. Deve suportar fonte redundante externa;

Capacidades
5.16. Deve Implementar no mínimo 90 Mpps;
5.17. Deve Implementar switch fabric de no mínimo 88 Gbps, ou seja, wirespeed;
5.18. Deve Implementar tabela de endereçamento para, no mínimo, 16.000 (dezesseis mil) endereços MAC;
5.19. Deve Implementar no mínimo 512 (quinhentos e doze) VLANs ativas - IEEE 802.1Q;

Protocolos
5.20. Deve Implementar IEEE 802.1Q;
5.21. Deve Implementar IEEE 802.1s;
5.22. Deve Implementar IEEE 802.3x;
5.23. Deve Implementar IEEE 802.1D;
5.24. Deve Implementar IEEE 802.1w;
5.25. Deve Implementar IEEE 802.3ad, 06 (seis) LAGs com 08 (oito) portas por LAG, inclusive entre portas de switches distintos da pilha;
5.26. Deve Implementar IGMP v1 e v2 e snooping;
5.27. Deve Implementar Broadcast Suppression por porta;
5.28. Deve Implementar Jumbo Frame 9000 bytes;
5.29. Deve Implementar o padrão IEEE 802.1ab e LLDP-MED;

Empilhamento
5.30. Deve permitir empilhar, no mínimo, 8 (oito) unidades;
5.31. Deve permitir o gerenciamento do switch e da pilha de switches através de endereço IP único;
5.32. Deve possuir 02 (duas) portas fixas ao chassi e específicas para empilhamento (stack), com desempenho mínimo de 10 (dez) Gbps por porta;
5.33. Deve suportar empilhamento redundante, através da ligação do último switch da pilha ao primeiro switch da pilha;
5.34. Deve permitir o empilhamento com o switch de acesso tipo I;

Roteamento
5.35. Deve implementar roteamento IP no mínimo para:
5.36. Rota estática;
5.37. RIP v1;
5.38. RIP v2;
5.39. OSPF;
5.40. OSPFv3;
5.41. Deve suportar no mínimo 60 (sessenta) rotas estáticas;
5.42. Deve suportar no mínimo 256 (duzentos e cinquenta e seis) rotas RIP;
5.43. Deve implementar DHCP Relay;

Qualidade de serviço
5.44. Deve implementar IEEE 802.1p;
5.45. Deve implementar Rate Limiting por porta;
5.46. Deve realizar classificação de tráfego: por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS;

5.47. Deve possuir a capacidade de associar um dispositivo autenticado por 802.1x a uma respectiva VLAN e ainda associar este dispositivo a política de filtragem de tráfego e de qualidade de serviço;
5.48. Deve possuir a capacidade de associar um dispositivo autenticado por endereço MAC a uma respectiva VLAN e ainda associar este dispositivo a política de filtragem de tráfego e de qualidade de serviço;
5.49. Deve implementar a remarcação do campo ToS (Type of Service);
5.50. Deve possuir no mínimo 6 (seis) filas de prioridade por porta;
5.51. Deve possuir algoritmo de enfileiramento Strict Priority e Weighted Round Robin;

Segurança

5.52. Deve permitir o controle de acesso a rede baseado no endereço MAC;
5.53. Deve ser possível configurar explicitamente os endereços MACs que podem ser aprendidos em uma porta do switch;
5.54. Deve ser possível informar, por porta do switch, a quantidade de endereços MACs que podem ser aprendidos dinamicamente, devendo permitir a configuração do valor mínimo para 1 (um) endereço MAC;
5.55. Deve implementar envio de trap SNMP quando ocorrer uma violação de filtro de MAC das situações acima;
5.56. Deve implementar IEEE 802.1X Port-Based Network Access Control de acordo com a RFC 3580;
5.57. Deve suportar autenticação via web para usuários visitantes, podendo a login ser feito na base local do switch ou através de Radius;
5.58. Deve suportar no mínimo 2 (dois) autenticações por porta;
5.59. Deve implementar autenticação de dispositivos através de endereço MAC, realizando a validação do endereço MAC em servidor Radius;
5.60. Deve implementar ACL ou outra funcionalidade de filtragem de tráfego por porta TCP/UDP de origem/destino, por endereço MAC de origem/destino, por endereço IP de origem/destino e por valor do campo ToS;
5.61. Deve implementar broadcast suppression por porta;
5.62. Deve implementar recurso para possibilitar que uma interface executando o protocolo Spanning Tree seja colocada no estado down quando a mesma receber um BPDU;
5.63. Deve implementar funcionalidade que bloqueie a operação de servidores DHCP inválidos (DHCP Spoof);
5.64. Deve implementar funcionalidade de Arp Spoof protection;
5.65. Deve implementar recurso de private VLAN ou protected port;

Gerenciamento

5.66. Deve implementar SSH V2;
5.67. Deve implementar SNMP v1, v2c e v3;
5.68. Deve suportar IPv6 para gerenciamento;
5.69. Deve implementar NTP ou SNTP;
5.70. Deve implementar Syslog Permitindo configurar no mínimo 05 (cinco) servidores de syslog distintos;
5.71. Deve implementar Radius e TACACS+;
5.72. Deve implementar mecanismo interno ao switch de teste de cabo metálico RJ-45 sendo possível obter, no mínimo, as seguintes informações:

- 5.73. Status operacional do cabo (ativo ou falha);
- 5.74. Tamanho aproximado do cabo;
- 5.75. Status de crosstalk ou falha de pinagem;

5.76. Deve implementar espelhamento de tráfego, inclusive entre portas de switches distintos da pilha. Deve permitir espelhar simultaneamente os frames recebidos e transmitidos;
5.77. Deve implementar Telnet;
5.78. Deve implementar TFTP ou FTP;
5.79. Deve Implementar CLI;
5.80. Deve implementar Sflow ou Netflow v5 ou Netflow v9;
5.81. Deve implementar RMON, 04 (quatro) grupos, sem utilização de probe externa;
5.82. Deve implementar gerenciamento por HTTP ou HTTPS através de acesso direto ao equipamento por web browser padrão;
5.83. Deve suportar, no mínimo, 02 (duas) Imagens do sistema operacional e 2 (dois) arquivos de configuração.

ITEM 6 - CABO DE EMPILHAMENTO CURTO PARA SWITCHES DE ACESSO

6.6.1. Deve ser compatível com os switches de acesso e do mesmo fabricante;

6.6.2. Deve possuir no mínimo 30 (trinta) centímetros de comprimento;
6.6.3. Devem ser fornecidos todos os acessórios para o empilhamento;

ITEM 7 - RACKS FECHADOS DE PISO 44Us

7.1. Deverá possuir 42U;
7.2. Deverá possuir no mínimo 600mm de largura;
7.3. Deverá possuir no mínimo 670mm de profundidade;
7.4. Deverá suportar no mínimo 500kg de carga estática;
7.5. Deverá possuir porta de vidro com espessura 5 mm;
7.6. Deverá permitir a inversão da abertura da porta frontal;
7.7. Deverá possuir portas laterais, frontal e traseira com sistema de fecho com chave;
7.8. Espessura das portas laterais de no mínimo 0.9 mm;
7.9. Deverá possuir 4(quatro) longarinas verticais, ajustáveis em profundidade, em aço galvanizado com espessura de 1,5mm;
7.10. As longarinas verticais deverão possuir furação 1/2U para fixação de equipamentos e acessórios através de porca gaiola M5;
7.11. Deverá vir com pintura eletrostática na cor preta;
7.12. Deverá vir com unidade de ventilação para Rack 19" com 4 ventiladores. Estrutura montada em bloco para fácil instalação e remoção, botão liga/desliga, led indicador de ligado, seletor de voltagem e fusível de proteção.
7.13. Deverá possuir no mínimo 2(duas) aberturas na base para entrada de cabos;
7.14. Deverá possuir indicação dos U's nos planos verticais;
7.15. Deverá possuir pés niveladores;
7.16. Deverá ser fornecido montado em pallet a fim de facilitar o transporte do produto;
7.17. Deverá atender as especificações da ANSI/EIA 310;
7.18. Incluir 04 (quatro) unidade de Régua de Tomadas Novo Padrão NBR 14136 2P+T de 10A, sendo cada uma delas com no mínimo 6 tomadas e fabricadas em chapa de aço com espessura de no mínimo 1,5mm 7.19. Kit com 180 (cento e oitenta) porca gaiola com parafuso compatível com o rack;
7.20. 02 (duas) bandeja frontal 1U;
7.21. Os racks devem ter garantia de pelo menos 12(doze) meses para defeitos de fabricação, contada da data de entrega do material.

ITEM 8 - SOFTWARE DE GERENCIAMENTO DE ATIVOS DE REDE

8.1. Deve prover uma interface gráfica para configuração e gerenciamento centralizado de todos os ativos de rede deste lote;
8.2. Deve estar licenciado para o gerenciamento de no mínimo 25 dispositivos IP;
A) Cada pilha de switches deve ser contabilizada como 1 (um) dispositivo gerenciado;
8.3. Deve ser do tipo cliente-servidor;
8.4. Pode ser composta por módulos integráveis, que permitam uma visualização gráfica e configuração remota de todos os equipamentos propostos, coleta de estatísticas SNMP e RMON, bem como apresentação da topologia da rede através de mapas;
8.5. Deve permitir a descoberta de equipamentos baseada em range de endereçamento IP ou em endereço de sub rede;
8.6. Deve permitir a classificação dos equipamentos descobertos por família de produtos ou sub rede IP;
8.7. Deve possuir capacidade de realizar backup e restore das configurações do switch;
8.8. Implantar monitoramento através dos protocolos SNMPv2c e SNMPv3;
8.9. Deve permitir que se visualizem os equipamentos de rede gerenciados e a topologia da rede;
8.10. Deve permitir descobrir a localização de usuário (s) ou dispositivo (s) na rede com base nos seguintes parâmetros:
8.11. Endereço IP ou intervalo de endereço IP;
8.12. Nome usuário autenticado por 802.1x;
8.13. Endereço MAC;
8.14. Deve permitir a visualização do status de cada porta bem como habilitá-la ou desabilitá-la;
8.15. Deve permitir a impressão, exportação e filtragem de alarmes e eventos;
8.16. Deve permitir à criação e o gerenciamento de políticas de controle de acesso à rede e de perfil de QoS para todos os switches ofertados.

8.17. Deverá permitir a criação de regras de permissão e negação de tráfego para controle de acesso à rede.
8.18. Deverá permitir a criação de regras de classificação e priorização de tráfego;
8.19. Deverá permitir a criação de regras de limitação de banda Rate Limit;
8.20. Deve permitir a aplicação destas regras nas portas dos switches de forma estática e/ou de forma dinâmica de acordo com o usuário/dispositivo autenticado através de 802.1x;
8.21. Deve permitir a integração do processo de autenticação 802.1x com servidores Radius;
8.22. Deve permitir a identificação do nome do usuário autenticado na porta do switch;
8.23. Deve permitir a criação e configuração de VLAN's.
8.24. Deve permitir a aplicação de configurações comuns a um conjunto de equipamentos, previamente estabelecidas (templates), de uma só vez.
8.25. Deve possibilitar o "reset" de um ou vários dispositivos simultaneamente.
8.26. Deve prover um inventário detalhado e organizado por tipo de equipamento.
8.27. Deve permitir comparar a configuração atual do equipamento com a que está armazenada no software e reportar quaisquer discrepâncias existentes.
8.28. Deve catalogar os atributos de cada dispositivo.
8.29. Deve informar a data e hora que a última configuração no equipamento foi salva.
8.30. Deve permitir a atualização do sistema operacional (IOS) para um ou vários dispositivos simultaneamente.
8.31. Deve possibilitar a gravação das configurações de dispositivos para cópia de segurança, tendo a possibilidade de ser feito agendamentos para essa tarefa.
8.32. Deve possibilitar a restauração de uma cópia de segurança e instalá-la em um dispositivo que apresentou problemas.
8.33. Deve ser possível a utilização em sistemas virtualizados VMware;
8.34. Caso a ferramenta necessite de banco de dados ou qualquer outro tipo de software, o mesmo deve ser fornecido de forma a garantir a solução completamente operacional.

ITEM 9 - SISTEMA DE ARMAZENAMENTO DE DADOS - STORAGE
9.1. Possuir 2 (duas) controladoras redundantes, ativas ou ativa-passiva e hot-pluggable, cada uma com 4 portas 10Gb short range iSCSI SFP+ já incluídos SFP+ 10Gb SW iSCSI
9.2. Memória cache total bruta com capacidade mínima de 8GB (oito gigabytes) por controladora;
9.3. Suportar discos das tecnologias SAS, NL-SAS, SSD e discos com a tecnologia SED;
9.4. Suportar no mínimo 256 (duzentos e cinquenta e seis) volumes lógicos (LUNs)
9.5. Deverá possuir a capacidade de expansão total de, no mínimo, 192 (cento e noventa) unidades de disco rígido do tipo SFF (SmallFormFactor) ou 96 (noventa e seis) unidades de disco rígido do tipo LFF (LargeFormFactor), sem a necessidade de expansão em sua capacidade de processamento, I/O ou memória;
9.6. Suportar a conexão de no mínimo 256 (duzentos e cinquenta e seis) Hosts ou superior, através de uma rede SAN fibrechannel;
9.7. Possuir ventiladores e fontes de alimentação, redundantes e hot-pluggable;
9.8. Implementar RAID níveis 1, 5, 6, 10, em qualquer combinação, processados pelo subsistema de discos do storage;
9.9. Recurso de eficiência energética onde as controladoras não deverão consumir energia quando não estiver em uso;
9.10. Possuir recurso que garante a integridade dos dados de escrita (write cache) armazenados na memória cache, em caso de falta de alimentação elétrica do subsistema primário;
9.11. Permitir total e plena disponibilidade das informações armazenadas, mesmo em face de atividades de manutenção técnica, tais como substituição de componentes, acréscimo de discos, ou atualização de microcódigos (firmware);
9.12. Devem ser fornecidos discos em tecnologia SAS de no mínimo 1.2TB (um ponto dois terabytes) e velocidade de 10.000 rotações por minuto (RPM), totalizando uma área útil em Raid 5 de no mínimo 3TiB;
9.13. Devem ser fornecidos discos em tecnologia SAS de no mínimo 2TB (dois terabytes) e velocidade de 7.200 rotações por minuto (RPM), totalizando uma área útil em Raid 5 de no mínimo 18TiB;
9.14. Os discos ofertados devem possuir 2 (duas) interfaces SAS (dual channel) com velocidade de 12Gb/s cada para SAS;
9.15. Cada gaveta de discos deve suportar conexão dual channel SAS e possuir 2 canais de back-end;
9.16. Possuir função de cópias físicas (Clone), onde o volume de origem deverá estar disponível para acesso, mesmo quando o clone está sendo criado;
9.17. Possuir função de criação de cópias (Snapshots) das informações armazenadas em seus volumes;

9.18. A área utilizada para criação do snapshot deve ter o seu uso liberado para gravação de dados após a deleção das cópias;
9.19. Implementar a criação de no mínimo 64 Snapshots e suportar a expansão para 512 Snapshots;
9.20. O storage deve permitir configurar discos hot-swap e Global Spare, bem como discos de spare dedicados para os níveis de RAID;
9.21. Possuir recurso nativo para análise e monitoração de performance e desempenho do storage;
9.22. Suportar recursos para recuperação de desastres (DR), como replicação para site de contingência;
9.23. Suportar os Sistemas Operacionais Windows Server 2012 ou superior, Linux RedHat Enterprise 6 ou superior, Suse Linux Enterprise 11 e 12, VMware 6.0 ou superior, utilizando o protocolo Fibre Channel;
9.24. Acompanhar software de gerenciamento do mesmo fabricante do storage, para administração centralizada, por meio de uma console de gerência web;
9.25. Ser capaz de definir os volumes lógicos de armazenamento (LUNs) e especificar quais servidores são autorizados a acessar esses volumes e quais as rotas de acesso (LUN masking e zoning);
9.26. Gerar alarmes/eventos em caso de falhas ou pré-falhas no subsistema e encaminha e-mail ao administrador de rede designado, comunicando essas ocorrências;
9.27. Possuir software para acesso as LUNs através de caminhos redundantes (multipath), possibilitando operar em caso de falha de uma controladora/HBA;
9.28. Possui fontes de alimentação com tensão de entrada de 100 - 240V e freqüência de 60Hz;
9.29. O fabricante do storage é compatível com as normas estabelecidas pela SNIA (Storage Networking IndustryAssociation) e prover interface de gerenciamento com os padrões SMI-S (Storage Management InitiativeSpecification) para gerenciamento através de ferramentas de gerência de storage que utilizem este padrão;
9.30. O fabricante do storage é participante do SNIA (Storage Networking IndustryAssociation) na qualidade de LargeMemberVoting, endereço eletrônico: www.snia.org/member_com/member_directory/;
9.31. Os softwares fornecidos em conjunto com o storage, devem possuir modalidade de licenciamento perpétuo, ou seja, não são cobrados quaisquer valores adicionais pelo uso do software durante e após o período do contrato.
9.32. Modelo próprio para rack padrão EIA de 19" devendo vir acompanhado de todas as peças e acessórios (trilhos, suportes, conectores, parafusos, etc.) necessários para fixação.

ITEM 10- SOLUÇÃO DE SISTEMA INFORMATIZADO DE BACKUP (SOFTWARE)

10.1. A solução deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução, incluindo retorno (rollback) de réplicas e replicação desde e até a infraestrutura virtualizada.
10.2. A solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.
10.3. Deverá garantir, no mínimo, a proteção de maquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware ou Hyper-V, conforme contratada.
10.4. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes.
10.5. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto.
10.6. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
10.7. Deverá prover a deduplicação e compressão das máquinas virtuais diretamente e durante a operação de backup.
10.8. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.
10.9. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.
10.10. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.
10.11. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreio de blocos modificados" (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
10.12. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:
10.12.1. Diretamente através de Storage Area Network (SAN);
10.12.2. Diretamente do storage, através do hypervisor I/O (Virtual Appliance);

10.12.3. Mediante uso da rede local (LAN);
10.13. Deverá poder manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço.
10.14. Deverá contar com tecnologia de deduplicação também para o ambiente de máquinas virtuais para gerar economia de espaço de armazenamento no repositório de backups sem a necessidade de hardware de terceiros (appliance de duplicadora).
10.15. Deverá proporcionar proteção quase contínua de dados (near-CDP), permitindo a mínimização dos Objetivos de Pontos de Recuperação (RPO).
10.16. Deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do arquivo de backup, armazenado no repositório de backup de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do backup, os quais obrigatoriamente deverão estar "deduplicados" e também "comprimidos".
10.17. 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.
10.18. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.
10.19. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar
10.20. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup.
10.21. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
10.22. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle.
10.23. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.
10.24. Deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.
10.25. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2010 sp1, 2013 e superiores, possam recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma.
10.26. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft Active Directory, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
10.37. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, tais como Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
10.38. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2010, sem a necessidade de agentes. (recuperação granular).
10.39. Deverá incluir ferramentas de recuperação de elementos individuais para Microsoft Exchange 2010- SP1 em diante, sem que seja necessário inicializar a máquina virtual a partir do backup e que possa ser extraído a frio (ex. mensagens, tarefas, contatos, etc.) e sem requerer infraestrutura intermediária (staging), fazer busca rápidas no servidor de e-mail;
10.40. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, gerando confiabilidade de 100% na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.).
10.41. Deverá permitir criar uma cópia da máquina virtual de produção, para criação de ambiente de homologação, teste, QA, etc; em qualquer estado anterior para a resolução de problemas, provas de procedimentos, capacitação, entre outros. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only).

10.42. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO3 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS.
10.43. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.
10.44. Deverá incluir suporte para VMware vCloud Director com visibilidade integrada da infraestrutura vCD no console de backup, fazendo backup de meta-dados e dos atributos associados com vApps e VMs, permitindo a recuperação diretamente ao vCD.
10.45. Deverá incluir um plug-in para VMware vSphere Web Client, afim de permitir o monitoramento da infraestrutura de backup diretamente do vSphere Web Client, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup.
10.46. Deverá operar em ambientes virtualizados através das soluções da VMware e Hyper-V, incluido:

a) VMware vSphere 5.5 e/ou Microsoft Hyper-V 2008-R2 e superiores.

10.47. Deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:

10.47.1. Microsoft Active Directory Server 2003 SP2 em diante
10.47.2. Microsoft Exchange Server 2010-SP1 em diante;
10.47.3. Microsoft SQL Server 2008 em diante;
10.47.4. Microsoft Sharepoint 2010 em diante;
10.47.5. Microsoft Project 2010 em diante;
10.47.6. Oracle Database 11g em diante.

10.48. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados.
10.49. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação.
10.50. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.
10.51. Deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de backup que esteja alojado em um provedor de serviços na nuvem (backup ou replicação na nuvem – cloud providers).
10.52. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual.
10.53. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos.
10.54. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas;
10.55. Suportar servidores proxy de backup virtuais ou físicos para backup de máquinas virtuais;
10.56. Deve estar homologado para o Oracle Database 11g e 12g nos sistemas operacionais Windows ou Linux sem a necessidade de instalação de agentes;
10.57. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;
10.58. Deve estar licenciado para utilização de no mínimo 1 biblioteca de fita com número idependente da quantidade de drives e slots operando simultânemente e com compartilhamento entre os jobs de backup;
10.59. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a contratante se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para a contratante
10.60. Deve dar suporte ao BitLooker

<u>Agentes Windows</u>

10.61. O licenciamento deve permitir a proteção de dados em computadores/servidores clientes baseados em sistema operacional Microsoft Windows em quantidade conforme definido no termo de referência.
Deverá prover capacidade de realização de backup, no mínimo, para as seguintes plataformas x86-64 bits:

10.61.1. Microsoft Windows 7 SP1
10.61.2. Microsoft Windows 8.x
10.61.3. Microsoft Windows 10
10.61.4. Microsoft Windows Server 2008 R2 SP1
10.61.5. Microsoft Windows Server 2012
10.61.6. Microsoft Windows Server 2012 R2

10.61.7. Microsoft Windows Server 2016

10.62. Os clientes baseados em Windows devem ter suporte para Microsoft BitLocker para backup e restauração

10.63. Permitir o backup e restauração de arquivos abertos, garantindo a integridade do backup.

10.64. Permitir restaurar o backup de recuperação de desastres para hardware similares ao original, também chamado de bare-metal restauração.

10.65. Deverá possuir a capacidade de criptografar os dados armazenados no backup, utilizando os algoritmos mais comuns de mercado, suportando a utilização de chaves de, pelo menos, 256 (duzentos e cinquenta e seis) bits.

10.66. Deve possuir a opção para ignorar blocos defeituosos (bad blocks).

10.67. Deverá permitir escolher se a criptografia será realizada no processamento dos dados, no tráfego de dados via rede ou no repositório de backup.

10.68. Deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do arquivo de backup, armazenado no repositório de backup de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do backup, os quais obrigatoriamente deverão estar "deduplicados" e também "comprimidos" para o Hypervisor Microsoft Hyper-V

10.69. 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 protegidas.

10.70. Todo serviço de migração das máquinas do repositório de backup até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.

10.71. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar

10.72. Deverá permitir a recuperação diretamente na nuvem Microsoft Azure;

10.73. Deverá possuir gerenciamento centralizado de backup e restauração via interface gráfica (GUI) e linha de comando (CLI):

10.74. Deverá permitir o agendamento de Jobs de backup dos clientes/servidor através da interface única da solução:

10.74.1. Permitir a execução de processos de backup segundo políticas a serem definidas (periodicidade, período de retenção, agendamento, tipo de backup – full e incremental)

10.74.2. Permitir definir prioridade de execução de jobs de backup;

10.74.3. Permitir programação de jobs de backup automatizadas em que sejam definidos prazos de retenção
das imagens.

10.74.4. Deverá prover monitoramento via interface gráfica e em tempo real dos jobs em execução.

10.74.4.1. Deverá gerar arquivos de logs para verificação das rotinas dos jobs.

10.75. Deverá suportar operações de backup e restauração em paralelo;

10.76. Deverá fazer uso de banco de dados para guardar o catálogo de jobs, arquivos e mídias dos backups 10.77. Deverá suportar backup e restauração de máquinas virtuais em VMware e Hyper-V, suportando backup de guest e backup de imagem;

10.78. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2010-SP1 e superiores, possam recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma.

10.79. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft Active Directory, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

10.80. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, tais como Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

10.81. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2010, sem a necessidade de agentes (recuperação granular).

10.82. Deverá incluir ferramentas de recuperação de elementos individuais para Microsoft Exchange 2010- SP1 em diante, sem que seja necessário inicializar a máquina virtual a partir do backup e que possa ser extraído a frio (ex. mensagens, tarefas, contatos, etc.) e sem requerer infraestrutura intermediária (staging), fazer busca rápidas no servidor de e-mail

10.83. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server.

Licenciamento

10.84. Atender as especificações mínimas previstas neste termo quanto às funcionalidades, integrações e compatibilidades com o ambiente físico e virtualizado da SEDICT para criação de backups e recuperação desses ambientes com o mínimo de indisponibilidade e reestruturação da parte física necessária, de forma que recupere, total e/ou granular, qualquer item assegurado por sua funcionalidade de backup / restauração e de replicação.

10.85. Cada licença de software licenciará um processador físico (CPU Socket) dos servidores hypervisor, do ambiente virtualizado (provedor/host das máquinas virtuais), e não deverá estar limitado à quantidade de máquinas virtuais ou quantidade de dados geridas e movimentadas por essa estrutura física. Para os servidores físicos as licenças devem ser individuais por equipamento e não deverá estar limitado à quantidade de dados geridas e movimentadas por este servidor.

ITEM 11 - SERVIDOR 14-CORE DO TIPO RACK COM CONEXÕES DE FIBRA

11.1. O equipamento deverá ser ofertado com dois processadores, sendo cada processador com pelo menos 14 núcleos de processamento operando a uma frequência de 2.2GHz (dois ponto dois giga-hertz) ou superior.

11.2. A configuração ofertada deverá prover índice de desempenho de pelo menos 1320 (um mil trezentos e vinte) pontos no teste SPECint2017rate Baseline, devidamente auditado pela Standard Performance Evaluation Corporation – SPEC (www.spec.org).

11.3. O equipamento deverá ser ofertado com no mínimo 256GB (duzentos e cinquenta e seis gigabytes) de memória padrão DDR4 operando a uma frequência de 2666 MT/s empregando módulos RDIMM com capacidade mínima de 16GB (dezesseis gigabytes) por módulo de memória.

11.4. O equipamento deverá suportar o emprego de tecnologias para correção de erros em memória, tais como Advanced ECC ou Online Spare.

11.5. Para armazenamento:

11.5.1. Deverá ser fornecido com pelo menos 02 (dois) discos HDD SSD, hot-plug com no mínimo de 480GB (quatrocentos e sessenta e oito), “hot pluggable/hot swap”, padrão SATA ou superior, configurados em RAID-1 por hardware e suporte.

11.5.2. Deverá ser fornecido com pelo menos 02 (dois) discos 600GB (seiscentos gigabytes), “hot pluggable/hot swap”, padrão SAS ou superior, configurados em RAID-1 por hardware e suporte.

11.5.3. Mínimo de 08 (oito) baias hot-plug ou hot-swap disponíveis para discos padrão SAS ou superior;

11.6. (uma) controladora de discos com suporte a RAID 0, 1, 5 e 6 com pelo menos 2GB de memória cache tipo flash (FBWC) ou protegida por bateria (BBWC);

11.6.1. Taxa de transferência de dados de 12Gb/s;

11.6.2. Suportar drives SSD (Solid-State Drive), HDD (Hard Disk Drive);

11.6.3. Possuir canais SAS 12 Gb/s, suficientes para suportar a quantidade máxima de discos do servidor;

11.7. Suportar pelo menos 3 slots PCIe 3.0 com barramento de pelo menos oito vias (x8). Ao menos um destes slots deverá ter barramento com dezesseis vias (x16).

11.8. No mínimo 3 portas USB 3.0.

11.9. Possuir placa de vídeo integrada ou instalada em slot de expansão, com suporte definição mínima de 1920 x 1200 @ 60 Hz (32 bpp).

11.10. Deverá possuir UEFI classe 2 desenvolvida pelo mesmo fabricante do equipamento para garantia de total compatibilidade com o software de gerenciamento.

11.11. Deverão possuir 02 (duas) portas de rede, com no mínimo 10 (dez) GigabitEthernet SFP+ integradas à placa principal ou instalada em slot de expansão, acompanhadas de transceivers.

11.11.1. Possuir interfaces de rede Gigabit Ethernet com no mínimo, 4 (quatro) portas RJ-45 1GbE;

11.12. Possuir pelo menos 01 (uma) porta de rede Ethernet para gerenciamento “out-of-band” independente das portas exigidas.

11.13. O equipamento deverá ser ofertado com fontes e ventiladores redundantes que suportem à instalação e substituição sem parada do equipamento, de modo que o servidor mantenha completa operacionalidade em caso de falha de qualquer um deles (fonte e ventilador). Deverá ser comprovado através de documentação do fabricante, que as fontes e ventiladores propostos são suficientes para suportar a configuração máxima do equipamento garantindo disponibilidade do mesmo através da redundância dos componentes (N+1 ou superior – onde N

representa o número mínimo necessário para suportar falha de pelo menos 1 componente tal seja fonte de alimentação, tal seja módulo de ventilação).
11.14. Deverá ser fornecido licenciamento de software para gerenciamento do servidor e seus componentes sem restrição de uso quanto às suas funcionalidades conforme especificadas neste edital.
11.15. Além do monitoramento e gestão da solução, o software deverá ser capaz de empregar configurações de maneira automática uma vez definidos os modelos de configuração para os componentes da solução.
11.16. Deverá permitir integração através de plug-ins com os sistemas de gerenciamento para ambiente virtualizado VMware vCenter Server na interface Web Client, bem como Microsoft System Center.
11.17. Deverá garantir autenticação simplificada de administradores através de single sign-on com os módulos de gerência do chassi, módulos de interconexão, servidores e suas respectivas consoles remotas. A autenticação deverá ser compatível com LDAP e Microsoft Active Directory.
11.18. Deverá permitir a definição de configurações para um servidor ou grupo de servidores com base em modelos de configuração que definem perfis de configuração para servidores (ethernet, fibre channel, volumes de armazenamento, Firmwares, BIOS/UEFI, ordem de inicialização ou boot, controladora RAID).
11.19. Os perfis de configuração deverão permitir a criação de modelos com a definição de versões mínimas de firmware e drivers de sistemas operacionais Windows e Linux para se manter conformidade de configuração entre os servidores do mesmo perfil, realizando o processo de atualização individual e em grupo, de maneira automática e programada.
11.20. Realizar instalação de sistemas operacionais Windows e Linux em servidores físicos e virtuais.
11.21. Deverá permitir a instalação, configuração e expansão de um cluster VMware através da interface de gerência e de maneira automatizada através da criação de modelos de configuração.
11.22. Permitir a instalação de sistemas operacionais em máquinas virtuais.
11.23. Atualizar drivers, utilitários e firmwares.
11.24. Configuração do hardware dos servidores, bem como seu respectivo módulo de gerência remota, BIOS, controladora RAID, rede e HBA.
11.25. Realizar o processo de instalação e configuração do hardware do servidor com ou sem o uso do protocolo PXE.
11.26. Executar o processo de instalação e configuração em múltiplos servidores simultaneamente.
11.27. O software deverá permitir a geração de relatórios de alertas, usuários, inventário de servidores, inventário de firmwares empregados, inventário de perfis de servidores.
11.28. O software deverá permitir que estes relatórios sejam exportados para arquivos CSV, Excel e PDF.
11.29. Deverá permitir acesso via navegador web com controle total das funções de vídeo, teclado, mouse (KVM) e mídias (USB, CD, DVD, arquivos de imagem ISO) da console remota do servidor instalado, com possibilidade de ligar, desligar e reiniciar, independente do funcionamento do sistema operacional, permitindo ainda que o administrador acesse e configure a BIOS/UEFI remotamente.
11.30. O acesso a console deverá ser simplificado com processo de única autenticação, também conhecido como single sign-on ou SSO, integrado com serviços de diretório LDAP e MS-AD.
11.31. A console deverá permitir o compartilhamento de uma mesma sessão de KVM para visualização e controle com pelo menos 4 (quatro) administradores, no mínimo, além de permitir captura de telas e gravação de vídeo para reprise quando necessário para diagnósticos e treinamentos.
11.32. Permitir a inicialização do servidor remotamente através de um arquivo de imagem ou dispositivo USB conectado na estação de trabalho do administrador.
11.33. Permitir integração com Microsoft Terminal Services quando o sistema operacional estiver totalmente carregado e disponível no servidor.
11.34. Permitir integração com VMware vCenter de modo que o gerenciamento e inventário também possa ser realizado através do vSphere Web Client com informações referentes aos hosts (nome do host, endereço IP do host, endereço IP do módulo de gerência integrado ao host, configuração de CPU, Memória, NICs, firmware), infraestrutura (energia, temperatura, módulos de ventilação, módulos de alimentação, módulo de gerência), rede (exibição de diagrama de rede com relação aos switches virtuais, adaptadores dos hosts, armazenamento (volumes de armazenamento, discos virtuais, HBAs com respectivos WWN, caminhos, conexão de VMs aos volumes), além de listar as versões de software/firmware em uso pelo host, controladoras de rede, HBA, RAID. Esta integração deverá permitir a redução os tempos de respostas a eventos de hardware através de ações automáticas pré-estabelecidas pelo administrador, tais como evacuação de máquinas virtuais em execução em um host que venha emitir alertas críticos. Manter estabilidade do ambiente e confiabilidade através do gerenciamento de firmwares empregados no ambiente, garantindo conformidade entre todos os hosts ESXi.
11.35. O servidor deverá ter altura máxima de 1U;
11.36. Alimentação elétrica:

11.36.1. Fontes redundantes, hot-pluggable e suporte a redundância 1+1.
11.36.2. A alimentação será disponibilizada em dois circuitos, sendo que o equipamento deverá manter a operacionalidade, em caso de falha de qualquer um deles.
11.36.3. Tensão de operação entre 100-127V e 200-240VCA.
11.36.4. Eficiência energética de no mínimo 94% (noventa e quatro por cento), (80Plus Platinum), quando em carga de 50% (cinquenta por cento), suficientes para operação do servidor em sua configuração máxima.
11.37. O servidor deverá estar em conformidade com a norma IEC 60950 (Safety of Information Technology Equipment incluiding Eletrical Business Equipment) para segurança do usuário contra incidentes elétricos ou combustão dos materiais elétricos.
11.38. A licitante deverá apresentar comprovação de compatibilidade através de HCLs dos respectivos fabricantes dos sistemas operacionais a seguir:
11.38.1. Sistema Operacional "Microsoft Windows Server versão 2012 R2 x64" ou superior em nível "Certified". A comprovação será realizada através do site oficial da Microsoft http://www.windowsservercatalog.com/
11.38.2. Sistema Operacional "VMware ESXi versão 6" ou superior. A comprovação será realizada através do site oficial da VMware http://www.vmware.com/resources/compatibility/
11.39. A licitante deverá fornecer todas as mídias necessários para instalação de drivers e software de gerência ou disponibilizar acesso para download através do site do fabricante indicado para o modelo e geração do equipamento ofertado.

ITEM 12 - IMPLANTAÇÃO DA SOLUÇÃO

12.1. Fornecer todos os cabos de ligação lógica e os componentes elétricos necessários à instalação e funcionamento dos componentes para suportar a instalação;
12.2. Todos os itens descritos nos requisitos técnicos deverão ser fornecidos e implementados segundo a necessidade da SEDICT, sem nenhum custo adicional;
12.3. A empresa vencedora deverá apresentar, em até 05 (cinco) dias corridos após a entrega do equipamento, projeto de implementação contendo prazos, gerenciamento de mudança, gerenciamento de riscos e plano de comunicação de acordo com as definições contidas no PMBOk do PMI, que deverá ser aprovado pela equipe técnica da SDE;
12.4. A empresa vencedora deverá executar o projeto de migração apresentado dentro do cronograma estipulado. Esta migração deverá ser executada exclusivamente por técnicos capacitados e habilitados a operar com a solução;
12.5. A empresa vencedora deverá fornecer todos os documentos e manuais necessários para garantir o bom funcionamento, suporte e manutenção dos equipamentos fornecidos;
12.6. A licitante deverá fornecer os seguintes serviços:
A) Instalação, configuração e tuning dos equipamentos ofertados;
B) Implementação de melhores práticas de mercado como VLANS.

ITEM 13 - OPERAÇÃO ASSISTIDA (APÓS IMPLEMENTAÇÃO DA SOLUÇÃO)

13.1. Nesta fase será realizada operação assistida por 80 (oitenta) horas, na modalidade on-site, na localidade da CONTRATANTE, fazendo o acompanhamento da operação da nova estrutura de rede, servidores e storage, executando o serviço local de suporte e transferindo o conhecimento para equipe da CONTRATANTE responsável pelo ambiente após este período.

CONSIDERAÇÕES FINAIS

1 - DESCRITIVO DETALHADO DOS SERVIÇOS

1.1. A fase inicial será de levantamento detalhado da conectividade física e lógica e configurações do Core da Rede, acesso e conectividade com servidores e storages.
1.2. Abaixo seguem etapas a serem concluídas:
1.2.1. Análise de documentação existente;
1.2.2. Análise de configurações dos switches atuais Core;
1.2.3. Análise de configurações dos switches atuais de Acesso;
1.3. Elaboração de Projeto Executivo contendo:
1.3.1. Diagramas em Blocos, Lógicos e Unifilares;
1.3.2. Plano de Endereçamento;
1.3.3. Plano de Segmentação (VLANs);
1.3.4. Plano de Roteamento;
1.3.5. Plano de Autenticação;

1.4. Elaboração de Plano de Implantação contendo:
1.4.1. Posicionamento de equipamentos e racks no data center e andares;
1.4.2. Interconexão entre o ambiente atual e novo ambiente para migração;
1.4.3 Cronograma para migração;
1.5. Após a validação do plano de migração e documentação pela CONTRATANTE, será iniciada a fase de migração do ambiente atual para os novos equipamentos e infra de rede, mantendo a mesma estrutura lógica, sendo considerado as seguintes fases:

1.5.1. Montagem e energização dos Novos equipamentos adquiridos (Core e Acesso), servidores e storage;
1.5.2. Configuração da conexão entre os Switches de Core e Acesso;
1.5.3. Configuração das portas dos Switches de acesso;
1.5.4. Transferência da fiação horizontal dos switches Core atuais para os novos Switches a serem fornecidos e existentes;
1.5.5. Configuração roteamento para o novo ambiente;
1.5.6. Configuração das Fibras de Conexão;
1.5.7. Testes de Conectividade;
1.5.8. Validação de funcionamento do roteamento, comunicação e serviços entre o ambiente atual e a ser adquirido durante a migração;
1.5.9. Validação de funcionamento da comunicação de rede e serviços após migração para os novos equipamentos
1.5.10. Validação da alta disponibilidade dos equipamentos em caso de falha;
1.5.11. Realizar testes básicos de conectividade entre os elementos e a avaliação se os serviços atuais (dos servidores / storages), para assegurar a funcionalidade após a migração e homologado junto a equipe da CONTRATANTE.
1.5.12. Configuração básica de endereçamento IP, sistema e dados SNMP;
1.5.13. Configuração do equipamento, com todas as funcionalidades solicitadas e necessárias para seu correto funcionamento: VLAN's, int vlan, Rotas estáticas ou dinâmicas, configuração SNMP.
1.5.14. 802.1X: configuração necessária para permitir que este ou encaminhe pacotes ou se autentique como estação a uma estrutura de autenticação já existente, limitando a configuração deste equipamento como cliente ou meio de passagem para o protocolo e com autenticação por usuário.
1.5.15. Migração dos firewalls e roteadores (Sistema WI-FI)

1.6. Ao final desta fase do projeto e antes do início da operação assistida, será fornecida toda documentação do Projeto, incluindo As Built e documentação do Resultado dos Testes.

2 - TRANSFERÊNCIA DE CONHECIMENTO

2.1. Deverá fornecer transferência de conhecimento para capacitar, ao menos, 03 (três) técnicos para plena utilização e configuração da solução ofertada, incluindo os softwares fornecidos;
2.2. O cronograma efetivo para a "Transferência de Conhecimento", será definido em conjunto com a SDE, após a assinatura do contrato;
2.3. A "Transferência de Conhecimento" será executada nas dependências da SDE durante a implementação da solução.