**INSTITUTO FEDERAL DE SANTA CATARINA**
**SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS**
EMITIDO EM 07/02/2018 11:29

## QUADRO DE ESPECIFICAÇÕES MÍNIMAS

**Licitação:** 23292.037737/2017-00 - PE 135/2017 - IFSC
**Assunto:** PERMANENTE INFORMÁTICA

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| **NÃO ASSOCIADO(S) A LOTE/GRUPO** | | | | | |
| 1 | CAB-CONSOLE-RJ45= CABO CONSOLE RJ45 | UNIDADE | 3 | 109,92 | 329,76 |
| 2 | CAB-CONSOLE-USB= CABO CONSOLE USB | UNIDADE | 13 | 152,26 | 1.979,38 |
| 3 | Cabo HDMI/RJ-45 para conexão do Cisco TelePresence SX20 existente no IFSC. Especificações mínimas: Cabo HDMI/RJ-45. Comprimento mínimo 2,5 mt. Conector 1x24 Macho. 1x19 HDMI (tipo A) macho Audio/Video. 1xRJ45 Macho para ligar Cisco TelePresence PrecisionHD 1080p Camera, Cisco | UNIDADE | 9 | 247,00 | 2.223,00 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 4 | Computador Desktop SFF Tipo Básico - Não acompanha Monitor 1. SISTEMA OPERACIONAL: Windows 10 Pro 64 a) A licença de uso (product key) do mesmo deve ser fixada em local visível ou gravada na memória flash da BIOS, possibilitando a leitura quando feito a reinstalação do Sistema Operacional. 2. PROCESSADOR: Intel Core i3-7100 ou equivalente AMD. Para equivalência de processadores considerar o uso (Desktop), o tamanho do cache (3MB) e a frequência do processador (3,9 GHz); 3. MEMÓRIA: Capacidade de 4GB DDR4 ou superior e velocidade padrão DDR4 2400MHz ou superior; 4. INTERFACE DE VÍDEO: Compatibilidade com DirectX 12 ou superior e OpenGL 4.1 ou superior. 5. Chipset corporativo; 6. DISCO RÍGIDO: SATA, com capacidade de 500 GB e rotação de 7200 rpm; 7. PORTAS: a) 6 portas USB sendo no mínimo 2 portas USB 3.0 ou superior; b) 1 entrada de vídeo VGA e 1 entrada de vídeo DP ou HDMI; c) 1 entrada RJ45; d) 1 conector de fone de ouvido e microfone (pode ser combo); 8. FONTE DE ALIMENTAÇÃO a) Fonte com chaveamento automático, suportando as tensões de entrada de 110/220V, interna; b) PFC ativo e potência máxima de 300W, suportando a configuração máxima do equipamento e eficiência de 85%; c) Frequência de 60Hz (com tolerância de 10%); d) Os cabos elétricos devem seguir a norma NBR 14136; 9. GABINETE a) Padrão SFF;; b) Tipo tool less que permita abertura do gabinete sem o uso de ferramentas; c) Suporte para dispositivos com cadeado e trava de cabo de chassi; d) Cor neutra (preto ou cinza) para gabinete, teclado e mouse; 10. TECLADO a) Com bloco numérico separado; b) Com Layout Português Brasil (ABNT2); c) Com ajuste de inclinação; d) Conectado por cabo USB ao computador; e) Do mesmo fabricante do equipamento. 11. MOUSE a) Tamanho padrão (não mini- mouse); b) Com 2 botões mais botão de rolagem (scroll); c) Modelo óptico; d) Conectado por cabo USB ao computador; e) Resolução de 800 dpi ou superior; f) Formato ergonômico ambidestro. 12. Fornecer mídia a cada empenho emitido pelo IFSC, independente da quantidade de computadores adquiridas. 13. GARANTIA e SUPORTE a) 60 (sessenta) meses, contada a partir do recebimento definitivo do equipamento, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante; b) O serviço de garantia será exigido da empresa vencedora. caberá a mesma prover o serviço de garantia, seja através de sua equipe de helpdesk, do fabricante ou rede autorizada pelo mesmo; c) O IFSC enviará a empresa vencedora a lista de equipamentos que apresentarem defeito, dentro do período de garantia, acompanhado do número de série de cada equipamento e a descrição do defeito, cabendo a esta empresa dar encaminhamento a solicitação. Não será aceito nenhum outro meio para a solicitação deste serviço de garantia; d) A empresa vencedora deverá fornecer endereço de e-mail e número de telefone para receber as solicitações de serviço de garantia do IFSC no momento da assinatura da ATA de REGISTRO DE PREÇOS. e) A partir do momento em que for aberto o chamado, via telefone ou mensagem eletrônica (e-mail), com os serviços solicitados, a empresa (licitante) vencedora terá 03 (três) dias úteis para atender ao chamado e até 30 dias corridos para a solução do defeito. O não atendimento ao chamado no prazo estipulado acarretará as penalidades contidas neste edital; f) Atendimento no local (on site); Caso seja necessário a retirada do equipamento com defeito, a empresa vencedora deverá prover a substituição por outro do mesmo modelo ou superior até que o equipamento consertado retorne para o IFSC; g) Caso o período para conserto seja superior a 30 dias corridos, a empresa vencedora deverá substituir o equipamento com defeito por um novo em definitivo; h) Comprovação através de catálogo ou declaração do fabricante que o modelo ofertado é da linha corporativa; 14. PROPOSTA a) Apresentar catálogo técnico oficial do produto que apresente as características técnicas em conformidade com as descritas no Termo de Referência deste edital, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; b) Caso a licitante envie catálogo sem estar grifado, conforme solicitado acima, a sua proposta será rejeitada não sendo aceito recurso para tal; c) Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; | UNIDADE | 500 | 2.357,66 | 1.178.830,00 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 5 | Computador Mini Desktop - Tipo Intermediário Não acompanha monitor; 1. SISTEMA OPERACIONAL: Windows 10 Pro 64 a) A licença de uso (product key) do mesmo deve ser fixada em local visível ou gravada na memória flash da BIOS, possibilitando a leitura quando feito a reinstalação do Sistema Operacional. 2. PROCESSADOR: Intel Core i5-7500T com Intel HD Graphics 630 ou equivalente AMD; Para equivalência de processadores considerar o uso (Desktop), o tamanho do cache (6M) e a frequência do processador (3,3GHz); 3. MEMÓRIA: Capacidade de 8GB DDR4 ou superior e velocidade padrão DDR4 2400MHz ou superior; 4. INTERFACE DE VÍDEO: Compatibilidade com DirectX 12 ou superior e OpenGL 4.1 ou superior. 5. Chipset corporativo 6. DISCO RÍGIDO: SATA, com capacidade de 500 GB e rotação de 7200 rpm, 2,5”; 7. PORTAS: a) 6 portas USB sendo no mínimo 2 portas USB 3.0 ou superior; b) 1 entrada de vídeo VGA e 1 entrada de vídeo DP ou HDMI; c) 1 entrada RJ45; d) 1 conector de fone de ouvido e microfone (pode ser combo); 8. FONTE DE ALIMENTAÇÃO a) Fonte com chaveamento automático, suportando as tensões de entrada de 110/220V, interna; b) PFC ativo e potência máxima de 90W, suportando a configuração máxima do equipamento com eficiência mínima de 85%; c) Frequência de 60Hz (com tolerância de 10%); d) Os cabos elétricos devem seguir a norma NBR 14136; 9. GABINETE a) Padrão Mini Desktop com volume máximo de 1.200 cm³; b) Tipo tool less que permita abertura do gabinete sem o uso de ferramentas; c) Suporte para dispositivos com cadeado e trava de cabo de chassi; d) Cor neutra (preto ou cinza) para gabinete, teclado e mouse; 10. TECLADO a) Com bloco numérico separado; b) Com Layout Português Brasil (ABNT2); c) Com ajuste de inclinação; d) Conectado por cabo USB ao computador; e) Do mesmo fabricante do equipamento. 11. MOUSE a) Tamanho padrão (não mini- mouse); b) Com 2 botões mais botão de rolagem (scroll); c) Modelo óptico; d) Conectado por cabo USB ao computador; e) Resolução de 800 dpi ou superior; f) Formato ergonômico ambidestro. 12. Fornecer mídia a cada empenho emitido pelo IFSC, independente da quantidade de computadores adquiridas. 13. Fornecer suporte para fixação em parede, mesa ou monitor. 14. GARANTIA e SUPORTE a) 60 (sessenta) meses, contada a partir do recebimento definitivo do equipamento, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante; b) O serviço de garantia será exigido da empresa vencedora. caberá a mesma prover o serviço de garantia, seja através de sua equipe de helpdesk, do fabricante ou rede autorizada pelo mesmo; c) O IFSC enviará a empresa vencedora a lista de equipamentos que apresentarem defeito, dentro do período de garantia, acompanhado do número de série de cada equipamento e a descrição do defeito, cabendo a esta empresa dar encaminhamento a solicitação. Não será aceito nenhum outro meio para a solicitação deste serviço de garantia; d) A empresa vencedora deverá fornecer endereço de e-mail e número de telefone para receber as solicitações de serviço de garantia do IFSC no momento da assinatura da ATA de REGISTRO DE PREÇOS. e) A partir do momento em que for aberto o chamado, via telefone ou mensagem eletrônica (e-mail), com os serviços solicitados, a empresa (licitante) vencedora terá 03 (três) dias úteis para atender ao chamado e até 30 dias corridos para a solução do defeito. O não atendimento ao chamado no prazo estipulado acarretará as penalidades contidas neste edital; f) Atendimento no local (on site); Caso seja necessário a retirada do equipamento com defeito, a empresa vencedora deverá prover a substituição por outro do mesmo modelo ou superior até que o equipamento consertado retorne para o IFSC; g) Caso o período para conserto seja superior a 30 dias corridos, a empresa vencedora deverá substituir o equipamento com defeito por um novo em definitivo; h) Comprovação através de catálogo ou declaração do fabricante que o modelo ofertado é da linha corporativa; 15. PROPOSTA a) Apresentar catálogo técnico oficial do produto que apresente as características técnicas em conformidade com as descritas no Termo de Referência deste edital, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; b) Caso a licitante envie catálogo sem estar grifado, conforme solicitado acima, a sua proposta será rejeitada não sendo aceito recurso para tal; c) Apresentar a “repetição” deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; | UNIDADE | 500 | 2.779,25 | 1.389.625,00 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 6 | COMUTADOR KVM USB 8 PORTAS (Especificações Mínimas): - Conexões para 8 computadores; - Inclusos conjunto de 8 cabos de no mínimo 1,8 metros (USB/PS2 para teclado/mouse e DB15 p/ video); - Interface USB compatível com 1.1 ou superior; - Conectores de porta PC: 8 x VGA HDB 15-pinos (fêmea); - Porta do console (todas fêmeas): 1 x USB tipo A / PS2 mouse 6-pinos mini din, 1 x USB tipo A / PS2 keyboard 6-pinos mini din, 1 VGA HDB 15-pinos (fêmea); - Porta do Console suporta tanto interface USB como PS/2; - Sistemas operacionais compatíveis: Windows 7 / XP, Linux, Unix e Mac; - Resolução de vídeo de até 2048 x 1536; - Controle OSD (On Screen Display) para fácil gerenciamento; - Modo de auto-scan ajustável para monitorar vários computadores; - LED Indicativos de Online e Seleção - Proteção por senha com auto timeout logout; - Auto detecção do número do banco quando cascateado; - Porta daisy-chain para cascatear até 16 níveis (128 computadores) a uma distância total de até 30 m; - Alerta de Beep para confirmação de chaveamento (habilita/desabilita) - Plug & play e hot-pluggable; - Montagem em Rack Padrão 19" (1U) - Kit de Montagem em Rack - Cerfiticações CE e FC - Entrada: 100~240 V AC - Adaptador de tensão externos 9 VDC, 1A; - Garantia: mínimo de 12 meses Modelo de referência: TK-804R | EQUIPAMENTO | 23 | 1.909,35 | 43.915,05 |
| 7 | Controle Remoto do Cisco TelePresence SX20 existente no IFSC. Especificações mínimas: Controle remoto TRC 5 para Cisco TelePresence SX20 IP Phone. Part Number Cisco CTS-RMT-TRC5=. Equipamento já existente no IFSC. | UNIDADE | 6 | 1.690,62 | 10.143,72 |
| 8 | Estabilizador de 1000VA bivolt com 8 tomadas. Características mínimas: potência nominal: 1000 Watts; tensão nominal de entrada: 115 / 127 / 220 V; faixa de tensão de entrada: 92 V – 150 V / 172 – 264 V; tensão nominal de saída: 115 V; frequência nominal: 60 Hz; corrente nominal de entrada: 9,4 / 8,5 / 4,9 A; variação admissível na saída: ± 6 %; proteção contra surtos de tensão: varistor; tempo de resposta: ≤ 6 semiciclos (50 ms); rendimento: > 92 %; não introduz distorção harmônica; método de seleção da tensão de entrada automática; tipo de acionamento: relé; comprimento do cabo de força: 90 cm; dimensões: 19,5 / 17 / 14 cm (Prof / Larg / Alt); produto na cor preta. Proteção contra sobrecorrente na entrada (fusível): fusível de 250 V, 12 A; tipo: ação lenta (5 x 20 mm). Painel traseiro: 8 tomadas de saída com novo padrão de tomadas brasileiro (NBR 14.373:2006); 1 porta fusíveis; cabo de força. Painel inferior: ventilação; proteção Fax/Modem. Garantia mínima de 12 meses. Modelo de referência: APC SOL1000G4BI-BR. | UNIDADE | 190 | 356,00 | 67.640,00 |
| 9 | FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) TIPO 1 Especificações Mínimas: 1. Características Gerais: 1.1. A solução de Firewall de Próxima Geração deve possuir as seguintes capacidades e características mínimas abaixo: 1.2. Características de Hardware Firewall: 1.2.1. Deve possuir capacidade de processamento de, no mínimo, 2 (dois) Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall e controle de aplicações ativas simultaneamente, considerando-se para fins de métrica ambientes de produção; 1.2.2. Deve possuir capacidade de processamento de, no mínimo, 2 (dois) Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente, considerando-se para fins de métrica ambientes de produção; 1.2.3. Suporte a, no mínimo, 1.000.000 (um milhão) de conexões simultâneas; 1.2.4. Suporte a, no mínimo, 12.000 (doze mil) novas conexões por segundo; 1.2.5. Possuir, no mínimo 12 (Doze) interfaces de rede 1 (um) Gbps RJ-45; 1.2.6. Possuir, no mínimo 4 (Quatro) interfaces de rede 1 (um) Gbps SFP; 1.2.7. Deve possuir 1 (uma) interface de rede Gigabit dedicada para gerenciamento; 1.2.8. Deve possuir 1 (uma) interface do tipo console ou similar; 1.2.9. Possuir fonte de energia AC redundante com ajuste automático de tensão para operação nas tensões de 100 a 240-VAC/60 Hz. 1.3. Características Gerais do Firewall: 1.3.1. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; 1.3.2. Deverá ser possível acessar o equipamento para aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem com alto nível de utilização através de isolamento do processamento de gerenciamento e do processamento do tráfego inspecionado; 1.3.3. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento; 1.3.4. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale; 1.3.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação; 1.3.6. O software deverá ser fornecido em sua versão mais recente e atualizada; 1.3.7. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS); 1.3.8. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: 1.3.8.1. Suporte a 1024 VLAN Tags 802.1q; 1.3.8.2. Agregação de links 802.3ad e LACP; 1.3.8.3. Roteamento multicast (IGMPv1/v2, PIM-SM, Bidir-PIM); 1.3.8.4. DHCP Relay; 1.3.8.5. DHCP Server; 1.3.8.6. Jumbo Frames; 1.3.8.7. Suportar sub-interfaces ethernet lógicas 1.3.8.8. Deve suportar os seguintes tipos de | EQUIPAMENTO | 1 | 108.509,08 | 108.509,08 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | NAT: 1.3.8.9. NAT dinâmico (Many-to-1); 1.3.8.10. NAT dinâmico (Many-to-Many); 1.3.8.11. NAT estático (1-to-1); 1.3.8.12. NAT estático (Many-to-Many); 1.3.8.13. NAT estático bidirecional 1-to-1; 1.3.8.14. Tradução de porta (PAT); 1.3.8.15. NAT de Origem; 1.3.8.16. NAT de Destino; 1.3.8.17. Suportar NAT de Origem e NAT de Destino simultaneamente. 1.3.8.18. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico; 1.3.8.19. NAT64 e NAT46; 1.3.9. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede; 1.3.10. Enviar log para sistemas de monitoração externos, simultaneamente; 1.3.11. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL; 1.3.12. Proteção anti-spoofing; 1.3.13. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); 1.3.14. Para IPv6, deve suportar roteamento estático e dinâmico; 1.3.15. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), Transparente, camada 2 (L2) e camada 3 (L3): 1.3.15.1. Modo Sniffer - para inspeção via porta espelhada do tráfego de dados da rede; 1.3.15.2. Modo transparente – para inspeção de dados em linha sem a necessidade de configuração dos equipamentos conectados; 1.3.15.3. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; 1.3.15.4. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas; 1.3.16. Suporte a configuração de alta disponibilidade Ativo/Passivo: 1.3.16.1. Em modo transparente; 1.3.16.2. Em layer 3; 1.3.17. A configuração em alta disponibilidade deve sincronizar: 1.3.17.1. Sessões; 1.3.17.2. Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, e objetos de rede; 1.3.17.3. Associações de Segurança das VPNs; 1.3.18. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link; 1.3.19. A configuração em alta disponibilidade deve possibilitar a instalação de cada membro, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP). 1.4. Controle por Política de Firewall: 1.4.1. Deverá suportar controles por zona de segurança; 1.4.2. Controles de políticas por porta e protocolo; 1.4.3. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações; 1.4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança; 1.4.5. Controle de políticas por País (geolocation) 1.4.6. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound); 1.4.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound); 1.4.8. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2; 1.4.9. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3; 1.4.10. Suporte a objetos e regras IPV6; 1.4.11. Suporte a objetos e regras multicast; 1.4.12. Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão; 1.5. Controle de Aplicações: 1.5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: 1.5.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos 1.5.3. Reconhecer pelo menos 3.200 (três mil e duzentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail; 1.5.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-tunnel, facebook chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, webex; 1.5.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo; 1.5.6. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.5.7. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. 1.5.8. Identificar o uso de táticas evasivas via comunicações criptografadas; 1.5.9. Atualizar a base de assinaturas de aplicações automaticamente; 1.5.10. Limitar a banda | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | (download/upload) usada por aplicações (rate limiting), baseado no IP de origem, usuários e grupos do LDAP/AD; 1.5.11. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; 1.5.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos; 1.5.13. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas; 1.5.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do ambiente da Contratante; 1.5.15. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL; 1.5.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.5.17. Deve alertar o usuário quando uma aplicação for bloqueada; 1.5.18. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações; 1.5.19. Deve possibilitar a diferenciação de tráfegos Peer2Peer (ex.:Bittorrent, emule, neonet) possuindo granularidade de controle/políticas para os mesmos; 1.5.20. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (ex.: AIM, Hangouts, Facebook Chat) possuindo granularidade de controle/políticas para os mesmos; 1.5.21. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o uso do chat e bloquear a chamada de vídeo; 1.6. Prevenção de Ameaças: 1.6.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e Anti-Malware integrados no próprio appliance de Firewall; 1.6.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos; 1.6.3. Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade; 1.6.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset; 1.6.5. Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão; 1.6.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura; 1.6.7. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens; 1.6.8. Deve permitir o bloqueio de vulnerabilidades; 1.6.9. Deve permitir o bloqueio de exploits conhecidos; 1.6.10. Deve incluir proteção contra ataques de negação de serviços; 1.6.11. Deverá possuir os seguintes mecanismos de inspeção de IPS: 1.6.11.1. Análise de padrões de estado de conexões; 1.6.11.2. Análise de decodificação de protocolo; 1.6.11.3. Análise para detecção de anomalias de protocolo; 1.6.11.4. IP Defragmentation; 1.6.11.5. Remontagem de pacotes de TCP; 1.6.11.6. Bloqueio de pacotes malformados; 1.6.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood e UDP flood; 1.6.13. Detectar e bloquear a origem de portscans; 1.6.14. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; 1.6.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS; 1.6.16. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.6.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.6.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações; 1.6.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; 1.6.20. Suportar bloqueio de arquivos por tipo; 1.6.21. Identificar e bloquear comunicação com botnets; 1.6.22. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: 1.6.22.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; 1.6.23. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação; 1.6.24. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas; 1.6.25. Os eventos devem identificar o país de onde partiu a ameaça; 1.6.26. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms; 1.6.27. Proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos; 1.6.28. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança; 1.7. Analise de Malwares Modernos: 1.7.1. Devido aos | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante; 1.7.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado; 1.7.3. Deve permitir selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, tipo de arquivo e todas estas opções simultaneamente; 1.7.4. Deve suportar a monitoração, detecção e prevenção em tempo real de arquivos trafegados nos seguintes protocolos HTTPS, FTP, HTTP, SMTP, IMAP, POP3 como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3; 1.7.5. Deve permitir especificar o tipo de arquivo, inclusive os comprimidos que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, vlans e outros objetos associados ao controle de acesso do ambiente protegido; 1.7.6. Permitir que seja definido o tamanho máximo dos arquivos a serem inspecionados; 1.7.7. Deve utilizar mecanismo de proteção baseado em reputação global em tempo-real, permitindo assim que sejam adotadas ações automáticas de alerta e bloqueio de arquivos suspeitos ou malwares já encontrados anteriormente; 1.7.8. O dispositivo não deve depender ou utilizar de forma exclusiva mecanismos de análise em ambiente virtualizado para que seja feita a detecção e o bloqueio de ameaças malwares em tempo-real; 1.7.9. A utilização de recursos de execução virtualizada, não deve depender da configuração manual de imagens ou escolha de versões específicas de sistemas operacionais; 1.7.10. Deve possui mecanismo blacklist para implementar controles customizados de forma automatizada; 1.7.11. Deve ossui mecanismo whitelist para implementar controles customizados de forma automatizada; 1.7.12. Deve possui capacidade para detecção de Malwares em comunicações de entrada e saída, incluindo a detecção de mecanismos de Comando e Control; 1.7.13. Deve identificar ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de ofuscação e indicadores de comprometimento automáticos; 1.7.14. Deve possuir tecnologia proprietária de execução para verificação de Malwares avançados inclusive mecanismos tipo sandbox; 1.7.15. Deve implementar a identificação e capacidade de controle de acesso em tempo real nos seguintes tipos de arquivo: MSEXE, 9XHIVE,DMG,DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG_PICT,MAYA,PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN, BINARY_DATA,BINHEX,EICAR,ELF,ISHIELD_MSI, MACHO, RPM, TORRENT, AMR, FFMPEG, FLAC, FLIC, FLV, IVR,MIDI,MKV,MOV,MPEG,OGG,PLS,R1M,REC,RIFF,RIFX,RMF,S3M,SAMI,SMIL,SWF,WAV,WEBM,7Z,ARJ,BZ,CPIO_CRC,CPIO_NEWC,CPIO_ODC,, JAR,LHA,MSCAB,MSSZDD,OLD_TAR,POSIX_TAR,RAR,SIS,SIT,ZIP,ZIP_ENC,ACCDB,HLP,MAIL,MDB,MDI,MNY,MSCHM,MSOLE2,MSWORD_MAC5,MWL,NEW_OFFICE,ONE,PST,RTF,TNEF,WAB,WP,WRI,XLW,XPS. Adicionalmente, deve implementar em tempo-real a inspeção, detecção e bloqueio autonomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos: 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC; 1.7.16. Deve implementar atualização a base de dados da Rede de Inteligência de forma automática; 1.7.17. Para recursos de análise virtualizada existente, deve ser mantido um histórico dos resultados de avaliações prévias de um arquivo e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite; 1.7.18. Dispor de múltiplos motores e mecanismos de detecção e prevenção para verificação de Malwares e códigos maliciosos incluindo: 1.7.18.1. Machine learning; 1.7.18.2. Reputação global; 1.7.18.3. Detecção customizada local por blacklist e regras customizadas de detecção de tráfego de rede; 1.7.18.4. Análise dinâmica (sandbox). 1.7.19. O processo de análise de comunicações, Malwares e sua prevenção deve ocorrer em tempo real, não sendo aceitas tecnologias que dependam de verificações que induzam latência suficiente para postergar a entrega de arquivos ao seu destino original; 1.7.20. Deve permitir o download dos malwares identificados a partir da própria interface de gerência; 1.7.21. Suportar a análise de arquivos executáveis, DLLs no ambiente controlado; 1.7.22. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class); 1.8. Filtro de URL: 1.8.1. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança; 1.8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local; 1.8.3. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; 1.8.4. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs; 1.8.5. Possuir pelo menos 80 categorias de URLs; 1.8.6. Permitir a criação de categorias de URLs customizadas; 1.8.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria; 1.8.8. Permitir a customização de página de bloqueio; 1.8.9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site); 1.9. Identificação de Usuários: 1.9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Active Directory e base de dados local; 1.9.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.9.3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2008, Windows Server 2012; 1.9.4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.9.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários; 1.9.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal). 1.10. Filtro de Dados: 1.10.1. Permitir a criação de filtros para arquivos e dados pré-definidos; 1.10.2. Os arquivos devem ser identificados por extensão e assinaturas; 1.10.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc); 1.10.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos; 1.10.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos; 1.10.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular. 1.11. Geo-Localização: 1.11.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados; 1.11.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos; 1.11.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas. 1.12. VPN: 1.12.1. Suportar VPN Site-to-Site 1.12.2. Suportar IPSec VPN; 1.12.3. A VPN IPSEc deve suportar: 1.12.4. 3DES; 1.12.5. Autenticação MD5 e SHA-1; 1.12.6. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 1.12.7. Algoritmo Internet Key Exchange (IKEv1 e v2); 1.12.8. AES 128, 192 e 256 (Advanced Encryption Standard); 1.12.9. Autenticação via certificado IKE PKI 1.12.10. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting. 2. Garantia 2.1. Todos os serviços baseados em assinaturas devem estar disponíveis por, no mínimo, 3 anos. 2.2. Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em até 3 dias úteis; 2.3. Visando atender à padronização que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas, de que trata o inciso I do artigo 15 da lei 8.666, de 21 de junho de 1993, os itens constantes deste grupo devem ser do mesmo fabricante dos equipamentos deste edital. - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. | | | | |
| 10 | Item: Firewall de Próxima Geração (NGFW) Tipo 2 Especificações Mínimas: 1. Características Gerais: 1.1. A solução de Firewall de Próxima Geração deve possuir as seguintes capacidades e características mínimas abaixo: 1.2. Características de Hardware Firewall: 1.2.1. Deve possuir capacidade de processamento de, no mínimo, 250 (duzentos e cinquenta) Mbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall e controle de aplicações ativas simultaneamente, considerando-se para fins de métrica ambientes de produção; 1.2.2. Deve possuir capacidade de processamento de, no mínimo, 125 (cento e vinte e cinco) Mbps para | EQUIPAMENTO | 4 | 16.335,48 | 65.341,92 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente, considerando-se para fins de métrica ambientes de produção; 1.2.3. Suporte a, no mínimo, 20.000 (vinte mil) de conexões simultâneas; 1.2.4. Suporte a, no mínimo, 5.000 (cinco mil) novas conexões por segundo; 1.2.5. Possuir pelo menos 8 (Oito) interfaces de rede 1 (um) Gbps; 1.2.6. Deve possuir 1 (uma) interface de rede Gigabit dedicada para gerenciamento; 1.2.7. Deve possuir 1 (uma) interface do tipo console ou similar; 1.2.8. Possuir fonte de energia AC com ajuste automático de tensão para operação nas tensões de 100 a 240-VAC/60 Hz; 1.3. Características Gerais do Firewall: 1.3.1. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; 1.3.2. Deverá ser possível acessar o equipamento para aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem com alto nível de utilização através de isolamento do processamento de gerenciamento e do processamento do tráfego inspecionado; 1.3.3. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento; 1.3.4. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale; 1.3.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação; 1.3.6. O software deverá ser fornecido em sua versão mais recente e atualizada; 1.3.7. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS); 1.3.8. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: 1.3.8.1. Suporte a 1024 VLAN Tags 802.1q; 1.3.8.2. Agregação de links 802.3ad e LACP; 1.3.8.3. Roteamento multicast (IGMPv1/v2, PIM-SM, Bidir-PIM); 1.3.8.4. DHCP Relay; 1.3.8.5. DHCP Server; 1.3.8.6. Jumbo Frames; 1.3.8.7. Suportar sub-interfaces ethernet lógicas 1.3.8.8. Deve suportar os seguintes tipos de NAT: 1.3.8.9. NAT dinâmico (Many-to-1); 1.3.8.10. NAT dinâmico (Many-to-Many); 1.3.8.11. NAT estático (1-to-1); 1.3.8.12. NAT estático (Many-to-Many); 1.3.8.13. NAT estático bidirecional 1-to-1; 1.3.8.14. Tradução de porta (PAT); 1.3.8.15. NAT de Origem; 1.3.8.16. NAT de Destino; 1.3.8.17. Suportar NAT de Origem e NAT de Destino simultaneamente. 1.3.8.18. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico; 1.3.8.19. NAT64 e NAT46; 1.3.9. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede; 1.3.10. Enviar log para sistemas de monitoração externos, simultaneamente; 1.3.11. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL; 1.3.12. Proteção anti-spoofing; 1.3.13. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); 1.3.14. Para IPv6, deve suportar roteamento estático e dinâmico; 1.3.15. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), Transparente, camada 2 (L2) e camada 3 (L3): 1.3.15.1. Modo Sniffer - para inspeção via porta espelhada do tráfego de dados da rede; 1.3.15.2. Modo transparente – para inspeção de dados em linha sem a necessidade de configuração dos equipamentos conectados; 1.3.15.3. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; 1.3.15.4. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas; 1.3.16. Suporte a configuração de alta disponibilidade Ativo/Passivo: 1.3.16.1. Em modo transparente; 1.3.16.2. Em layer 3; 1.3.17. A configuração em alta disponibilidade deve sincronizar: 1.3.17.1. Sessões; 1.3.17.2. Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, e objetos de rede; 1.3.17.3. Associações de Segurança das VPNs; 1.3.18. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link; 1.3.19. A configuração em alta disponibilidade deve possibilitar a instalação de cada membro, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP). 1.4. Controle por Política de Firewall: 1.4.1. Deverá suportar controles por zona de segurança; 1.4.2. Controles de políticas por porta e protocolo; 1.4.3. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações; 1.4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança; 1.4.5. Controle de políticas por País (geolocation) 1.4.6. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound); 1.4.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound); 1.4.8. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2; 1.4.9. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3; 1.4.10. Suporte a objetos e regras IPV6; 1.4.11. Suporte a objetos e regras multicast; 1.4.12. Deve suportar no mínimo os seguintes tipos | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão; 1.5. Controle de Aplicações: 1.5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: 1.5.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos 1.5.3. Reconhecer pelo menos 3.200 (três mil e duzentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail; 1.5.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-tunnel, facebook chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, webex; 1.5.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo; 1.5.6. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.5.7. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. 1.5.8. Identificar o uso de táticas evasivas via comunicações criptografadas; 1.5.9. Atualizar a base de assinaturas de aplicações automaticamente; 1.5.10. Limitar a banda (download/upload) usada por aplicações (rate limiting), baseado no IP de origem, usuários e grupos do LDAP/AD; 1.5.11. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; 1.5.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos; 1.5.13. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas; 1.5.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do ambiente da Contratante; 1.5.15. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL; 1.5.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.5.17. Deve alertar o usuário quando uma aplicação for bloqueada; 1.5.18. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações; 1.5.19. Deve possibilitar a diferenciação de tráfegos Peer2Peer (ex.:Bittorrent, emule, neonet) possuindo granularidade de controle/políticas para os mesmos; 1.5.20. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (ex.: AIM, Hangouts, Facebook Chat) possuindo granularidade de controle/políticas para os mesmos; 1.5.21. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o uso do chat e bloquear a chamada de vídeo; 1.6. Prevenção de Ameaças: 1.6.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e Anti-Malware integrados no próprio appliance de Firewall; 1.6.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos; 1.6.3. Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade; 1.6.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset; 1.6.5. Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão; 1.6.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura; 1.6.7. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens; 1.6.8. Deve permitir o bloqueio de vulnerabilidades; 1.6.9. Deve permitir o bloqueio de exploits conhecidos; 1.6.10. Deve incluir proteção contra ataques de negação de serviços; 1.6.11. Deverá possuir os seguintes mecanismos de inspeção de IPS: 1.6.11.1. Análise de padrões de estado de conexões; 1.6.11.2. Análise de decodificação de protocolo; 1.6.11.3. Análise para detecção de anomalias de protocolo; 1.6.11.4. IP Defragmentation; 1.6.11.5. Remontagem de | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | pacotes de TCP; 1.6.11.6. Bloqueio de pacotes malformados; 1.6.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood e UDP flood; 1.6.13. Detectar e bloquear a origem de portscans; 1.6.14. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; 1.6.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS; 1.6.16. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.6.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.6.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações; 1.6.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; 1.6.20. Suportar bloqueio de arquivos por tipo; 1.6.21. Identificar e bloquear comunicação com botnets; 1.6.22. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: 1.6.22.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; 1.6.23. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação; 1.6.24. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas; 1.6.25. Os eventos devem identificar o país de onde partiu a ameaça; 1.6.26. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms; 1.6.27. Proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos; 1.6.28. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança; 1.7. Analise de Malwares Modernos: 1.7.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante; 1.7.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado; 1.7.3. Deve permitir selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, tipo de arquivo e todas estas opções simultaneamente; 1.7.4. Deve suportar a monitoração, detecção e prevenção em tempo real de arquivos trafegados nos seguintes protocolos HTTPS, FTP, HTTP, SMTP, IMAP, POP3 como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3; 1.7.5. Deve permitir especificar o tipo de arquivo, inclusive os comprimidos que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, vlans e outros objetos associados ao controle de acesso do ambiente protegido; 1.7.6. Permitir que seja definido o tamanho máximo dos arquivos a serem inspecionados; 1.7.7. Deve utilizar mecanismo de proteção baseado em reputação global em tempo-real, permitindo assim que sejam adotadas ações automáticas de alerta e bloqueio de arquivos suspeitos ou malwares já encontrados anteriormente; 1.7.8. O dispositivo não deve depender ou utilizar de forma exclusiva mecanismos de análise em ambiente virtualizado para que seja feita a detecção e o bloqueio de ameaças malwares em tempo-real; 1.7.9. A utilização de recursos de execução virtualizada, não deve depender da configuração manual de imagens ou escolha de versões específicas de sistemas operacionais; 1.7.10. Deve possui mecanismo blacklist para implementar controles customizados de forma automatizada; 1.7.11. Deve possui mecanismo whitelist para implementar controles cust mizados de forma automatizada; 1.7.12. Deve possui capacidade para detecção de Malwares em comunicações de entrada e saída, incluindo a detecção de mecanismos de Comando e Control; 1.7.13. Deve identificar ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de ofuscação e indicadores de comprometimento automáticos; 1.7.14. Deve possuir tecnologia proprietária de execução para verificação de Malwares avançados inclusive mecanismos tipo sandbox; 1.7.15. Deve implementar a identificação e capacidade de controle de acesso em tempo real nos seguintes tipos de arquivo: MSEXE, 9XHIVE,DMG,DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG_PICT,MAYA,PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN, BINARY_DATA,BINHEX,EICAR,ELF,ISHIELD_MSI, MACHO, RPM, TORRENT, AMR, FFMPEG, FLAC, FLIC, FLV, IVR,MIDI,MKV,MOV,MPEG,OGG,PLS,R1M,REC,RIFF,RIFX,RMF,S3M,SAMI,SMIL,SWF,WAV,WEBM,7Z,ARJ,BZ,CPIO_CRC,CPIO_NEWC,CPIO_ODC,, JAR,LHA,MSCAB,MSSZDD,OLD_TAR,POSIX_TAR,RAR,SIS,SIT,ZIP,ZIP_ | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | ENC,ACCDB,HLP,MAIL,MDB,MDI,MNY,MSCHM,MSOLE2,MSWORD_MAC5 ,MWL,NEW_OFFICE,ONE,PST,RTF,TNEF,WAB,WP,WRI,XLW,XPS. Adicionalmente, deve implementar em tempo-real a inspeção, detecção e bloqueio autonomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos: 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC; 1.7.16. Deve implementar atualização a base de dados da Rede de Inteligência de forma automática; 1.7.17. Para recursos de análise virtualizada existente, deve ser mantido um histórico dos resultados de avaliações prévias de um arquivo e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite; 1.7.18. Dispor de múltiplos motores e mecanismos de detecção e prevenção para verificação de Malwares e códigos maliciosos incluindo: 1.7.18.1. Machine learning; 1.7.18.2. Reputação global; 1.7.18.3. Detecção customizada local por blacklist e regras customizadas de detecção de tráfego de rede; 1.7.18.4. Análise dinâmica (sandbox). 1.7.19. O processo de análise de comunicações, Malwares e sua prevenção deve ocorrer em tempo real, não sendo aceitas tecnologias que dependam de verificações que induzam latência suficiente para postergar a entrega de arquivos ao seu destino original; 1.7.20. Deve permitir o download dos malwares identificados a partir da própria interface de gerência; 1.7.21. Suportar a análise de arquivos executáveis, DLLs no ambiente controlado; 1.7.22. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class); 1.8. Filtro de URL: 1.8.1. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança; 1.8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local; 1.8.3. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; 1.8.4. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs; 1.8.5. Possuir pelo menos 80 categorias de URLs; 1.8.6. Permitir a criação de categorias de URLs customizadas; 1.8.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria; 1.8.8. Permitir a customização de página de bloqueio; 1.8.9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site); 1.9. Identificação de Usuários: 1.9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Active Directory e base de dados local; 1.9.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.9.3. Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2008, Windows Server 2012; 1.9.4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.9.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários; 1.9.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal). 1.10. Filtro de Dados: 1.10.1. Permitir a criação de filtros para arquivos e dados pré-definidos; 1.10.2. Os arquivos devem ser identificados por extensão e assinaturas; 1.10.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc); 1.10.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos; 1.10.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos; 1.10.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular. 1.11. Geo-Localização: 1.11.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados; 1.11.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos; 1.11.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas. 1.12. VPN: 1.12.1. Suportar VPN Site-to-Site 1.12.2. Suportar IPSec VPN; 1.12.3. A VPN IPSEc deve suportar: 1.12.4. 3DES; 1.12.5. Autenticação MD5 e SHA-1; 1.12.6. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 1.12.7. | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | Algoritmo Internet Key Exchange (IKEv1 e v2); 1.12.8. AES 128, 192 e 256 (Advanced Encryption Standard); 1.12.9. Autenticação via certificado IKE PKI 1.12.10. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting. 2. Garantia 2.1. Todos os serviços baseados em assinaturas devem estar disponíveis por, no mínimo, 3 anos. 2.2. Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em até 3 dias úteis; 2.3. Visando atender à padronização que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas, de que trata o inciso I do artigo 15 da lei 8.666, de 21 de junho de 1993, os itens constantes deste grupo devem ser do mesmo fabricante dos equipamentos deste edital. - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. | | | | |
| 11 | Impressora: Principais características da Impressora 3D: • Impressão 3D em dois materiais com duas cabeças de impressões; • Espessura da camada de impressão mínima de 100 mícrons; • Controle de camadas de impressão de 100 a 250 mícros; • Impressão 3D em material Nylon; ABS; PLA; • O equipamento deve acompanhar Software de impressão; • Estrutura do equipamento deve ser acrílico, alumínio ou aço. • Deve ser fornecido 2kg de cada material ABS, PLA e Nylon junto ao equipamento • Bico extrusor para filamento de 1,75mm e diâmetro saída 0,4mm ou 0,3mm. • Suporte em Português – Todo o suporte a venda e pós-venda bem como o treinamento de utilização da impressora em Português do Brasil. Especificações técnicas da Impressora 3D: • Tecnologia de impressão: FDM – Fused Deposition Modeling – Modelagem por deposição de termoplástico fundido; • Menor resolução de camada: 100 Mícrons; • Diâmetro do filamento: 1.75 mm; • Compatibilidade do filamento: Filamento de ABS; PLA e Nylon; • Temperatura de trabalho: 15-32°C; • Volume de impressão máximo (Aproximado): 23cm X 22,5cm X 205cm; • Arquivos Suportados: STL, OBJ, THING (pelo menos); • Sistemas operacionais suportados para instalação: WINDOWS (7+), MAC OS X (10.7+) ou LINUX (UBUNTU 12.04+); • Elétrica: 100–240 V, ~4 AMPS, 50–60 HZ; • Conectividade: USB, SD CARD; • Garantia: 12 meses. | UNIDADE | 5 | 16.449,00 | 82.245,00 |
| 12 | IMPRESSORA DE ETIQUETAS; TRANSFERÊNCIA TÉRMICA E TÉRMICA DIRETA; 200DPI ,102MM POR SEGUNDO; USB, RS-232 E CENTRONIC PARALLEL; TEXTOS, IMAGENS, CÓDIGOS DE BARRA 1D, 2D E QR CODE;ENTRADA 110/220V\, SISTEMA OPERACIONAL WINDOWS 98/NT 4.0/2000/XP 12 MESES DE GARANTIA. | UNIDADE | 5 | 1.095,00 | 5.475,00 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 13 | INJETOR PoE --> Características técnicas mínimas: 1. Injetor PoE (power injector) para alimentação de dispositivos PoE onde não há switch com esta tecnologia; 2. Deve permitir o fornecimento de energia capaz de alimentar o Ponto de Acesso Interno Tipo 01 deste processo com 100% de operação; 3. Deve possuir 2 portas RJ-45 fêmea, uma para conectar ao switch não PoE, outra para fornecer energia e dados para o ponto de acesso. Ambas as portas devem operar em Gigabit; 4. Deve acompanhar cabos e acessórios para o seu perfeito funcionamento; 5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V/220V com comutação automática e frequência de 60Hz. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136; 6. A garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento, deverá ser pelo período mínimo de 36 meses; - A garantia deve incluir a reposição de equipamentos on site nos locais especificados neste termo de referência. - Os serviços serão solicitados mediante a abertura de um chamado, via chamada telefônica 0800, e-mail, website ou chat da licitante vencedora, e, constatada a necessidade, a mesma deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao IFSC; - O atendimento aos chamados deve ser realizado em até 1 dia útil a partir da abertura do chamado. - A resolução do problema e/ou defeito registrado deverá ocorrer, no máximo, em 15 dias corridos a partir da abertura do chamado. - Caso seja necessário a substituição do equipamento, a mesma deverá ser realizada em até 30 dias corridos, a partir da constatação pela equipe técnica da licitante vencedora, dentro do prazo de 15 dias conforme descrito no item anterior; - A licitante vencedora deve indicar, na assinatura da Ata de Registro de Preços, os procedimentos para abertura de suporte técnico; - A garantia iniciará sua contagem a partir da data de emissão da NF dos equipamentos, serviços ou licenças. - Prazo de entrega de produtos: no máximo 90 (noventa) dias corridos a partir da emissão de Autorização de Fornecimento pelo IFSC; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas não sendo aceitos equipamentos com caixas violadas. | UNIDADE | 45 | 595,34 | 26.790,30 |
| 14 | SWITCH 24 PORTAS GIGABIT L3 CORE Especificações Mínimas: 1. Comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve ser fornecido com 24 (vinte e quatro) portas 100/1000BaseT, conectores RJ-45 fornecido diretamente no equipamento; 3. Deve ser fornecido com 4 slots SFP para conexão de transceivers SFP para fibras ópticas multimodo e monomodo. Estas portas devem ser de uso simultâneo com as portas do item anterior e não serão aceitas interfaces do tipo combo; 4. Deve possuir 28 portas ethernet ativas simultaneamente, não incluindo interfaces de empilhamento; 5. Deve possuir capacidade de vazão de pelo menos 41 mpps, com switching bandwidth de 88 Gbps Full-duplex; 6. Deve suportar empilhamento através de interfaces dedicadas, com velocidade mínima de 160 Gbps Full duplex na pilha, configurado em forma de anel, formando pilhas de pelo menos 4 unidades. Deve-se utilizar portas específicas para este fim; A porta e cabo de empilhamento devem ser fornecidas neste processo. Deve empilhar com switches PoE e não PoE. Os switches PoE devem prover alimentação conforme o padrão 802.3at, fornecendo até 30W por porta. Deve permitir a criação de links agrupados virtualmente (link aggregation) utilizando portas de diferentes switches da pilha; 7. Deve possuir porta de console para total gerenciamento local, com conector RS-232, RJ-45 ou USB; 8. O equipamento deve permitir sua configuração automática com base em outro equipamento da rede, sem intervenção humana, permitindo a rápida substituição do equipamento. Ao ser ligado, o equipamento deve buscar esta configuração em outro equipamento da rede, utilizando-se para isso parâmetros fornecidos pelo DHCP; 9. Deve possuir Jumbo Frame de pelo menos 9000 bytes; 10. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, e deve permitir a criação de no mínimo 512 VLANs com 4094 VLAN ID; 11. O equipamento deve suportar a criação de 8 rotas estáticas e protocolos de roteamento RIPv1 e RIPv2 para criação de pequenos backbones, suportando upgrade futuro para suportar roteamento OSPF e BGP em IPv4 e IPv6, estando o hardware totalmente preparado para o mesmo 12. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring); 13. Deve permitir a criação de links agrupados virtualmente (link aggregation); 14. Deve possuir funcionalidade de LLDP conforme o padrão IEEE 802.1ab, que permita o auto descobrimento do equipamento conectado na porta do switch. A detecção do equipamento conectado deve ocorrer de forma automática; 15. Deve possuir IGMP snooping com pelo menos 256 grupos para controle de tráfego de multicast; 16. Deve identificar automaticamente portas em que telefones IP estejam conectados e associá-las automaticamente a VLAN de voz; 17. Deve possuir Spanning Tree padrão IEEE 802.1w (Rapid Spanning Tree), IEEE 802.1s (Multiple Spanning Tree) com filtros BPDU e spanning tree por | EQUIPAMENTO | 15 | 27.864,97 | 417.974,55 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | vlan. Deve implementar pelo menos 32 instâncias; 18. Deve possuir priorização de pacotes (QoS) com 4 filas de prioridade por porta. Deve implementar a classificação de pacotes com base em regras de ACL; 19. Deve possuir autenticação IEEE 802.1x com assinalamento de VLAN por usuário e Guest VLAN para usuários não autenticados. Para usuários sem cliente IEEE 802.1x instalado, deve possuir um portal Web interno ao equipamento para autenticação; 20. Deve possuir autenticação IEEE 802.1x de múltiplos usuários por porta, para o caso de links com switches não gerenciáveis. Apenas o tráfego dos usuários que se autenticarem será permitido; 21. Deve implementar criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes a senha; 22. Deve possuir MTBF de no mínimo 661000 horas; 24. Deve implementar Internet Group Management Protocol (IGMP) v1, v2, v3 snooping para IPv4: limitar o trafego de vídeo somente para os solicitantes; 25. Deve permitir RSPAN (Remote Switch Port Analyzer) para monitoramento remoto de portas na camada 2 de qualquer outro switch da mesma rede. 26. Deve permitir o monitoramento de RF (Radio Frequência) (item pode ser adquirido futuramente através de licenciamento, não necessita estar presente nesta especificação); 27. Deve permitir configurar quantos endereços MAC podem ser aprendidos em uma porta, e permitir configurar qual ação será tomada quando esta regra for quebrada; 28. Deve armazenar no mínimo 32000 endereços MAC; 29. Deve suportar o gerenciamento de, no mínimo, 25 pontos de acesso sem fio nativamente. As licenças de access points não precisam ser fornecidas neste processo; 30. Deve suportar a criação de 64 WLANs; 31. Deve suportar o gerenciamento dos pontos de acesso sem fio série Aironet do fabricante Cisco já existentes neste orgão. 32. Deve permitir evitar loops acidentais na topologia física, identificando BPDU juntamente com o protocolo Spanning-Tree; 33. Deve ser compatível com no mínimo os seguintes padrões IEEE: IEEE 802.1as, IEEE 802.1s, IEEE 802.1w,IEEE 802.11,IEEE 802.1x,IEEE 802.1x-Rev, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3bz, IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports, IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS prioritization, IEEE 802.1Qat Stream Reservation Protocol, IEEE 802.1Qav, IEEE 802.1Q VLAN, IEEE 802.3 10BASE-T specification, IEEE 802.3u 100BASE-TX specification, IEEE 802.3ab 1000BASE-T specification, IEEE 802.3z 1000BASE-X specification 34. Deve permitir a criação de listas de acesso (ACLs) em IPv4, internamente ao equipamento, baseadas em endereço IP de origem, endereço IP de destino, protocolo, portas TCP, UDP, ICMP, IGMP, campo DSCP, campo ToS e dia e hora. Deve ser possível definir ACL por VLAN e habilitar o log da ACL; 35. Deve implementar IPv6 com as seguintes RFCs: 1981, 2373, 2460, 2461, 2462 e 2463; 36. Deve permitir a configuração de DHCP Server e DHCP Relay com suporte a múltiplas VLANs simultaneamente; 37. Deve possuir DHCP Snooping para eliminação de falsos servidores de DHCP; 38. Deve possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC, de forma a evitar ataques na rede; 30. Deve possuir o protocolo "Network Time Protocol" (NTP), autenticado, em IPv4 e IPv6, para a sincronização do relógio com outros dispositivos de rede, garantindo a alta efetividade e segurança na troca de mensagens com os servidores de tempo; 40. Deve ser fornecido cabo console RJ45 original com no mímino 1,5m; 41. Deve permitir configuração/administração remota através de SSH e SNMPv3; 42. Deve permitir a criação de três níveis de administração e configuração do switch. Permitir a autenticação de usuário de gerência em servidor RADIUS e TACACS+; 43. Deve implementar tecnologia para monitoramento de tráfego baseado em IPFIX, Netflow, Sflow ou Netstream, garantindo alta visibilidade do tráfego de rede. Caso a análise seja feita por amostragem, deve ser suportada amostragem de 1 a cada 32 pacotes; 44. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática. Deve suportar fonte de alimentação redundante. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136; 45. Deve permitir o envio de mensagens geradas pelo sistema em servidor externo (syslog), indicando a hora exata do acontecimento; 46. Gabinete padrão para montagem em rack de 19", com altura máxima de 1U, incluindo todos os acessórios para o perfeito funcionamento; 47. A garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento, deverá ser pelo período mínimo de 36 meses; - A garantia deve incluir o envio de equipamentos de reposição que deverão ser entregues nos locais especificados neste termo de referência. - Os serviços serão solicitados mediante a abertura de um chamado, via chamada telefônica 0800, e-mail, website ou chat da licitante vencedora, e, constatada a necessidade, a mesma deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante; - O atendimento aos chamados deve ser realizado em até um dia útil a partir da abertura do chamado. - A resolução do problema e/ou defeito registrado deverá ocorrer, no máximo, em 15 dias corridos a partir da abertura do chamado. - Caso seja necessário a | | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | substituição do equipamento, a mesma deverá ser realizada em até 30 dias corridos, a partir da constatação pela equipe técnica da licitante vencedora, dentro do prazo de 15 dias conforme descrito no item anterior; - A licitante vencedora deve indicar, na assinatura da Ata de Registro de Preços, os procedimentos para abertura de suporte técnico; - A licitante vencedora deve possuir, no momento da assinatura da Ata de Registro de Preços, pelo menos 1 (um) profissional com certificação técnica específica da tecnologia empregada (SWITCH) emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; Comprovação através da apresentação da certificação. - A contratante poderá solicitar o escalonamento de incidentes ao fabricante do equipamento quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware; - A garantia iniciará sua contagem a partir da data de emissão da NF dos equipamentos, serviços ou licenças. - Prazo de entrega de produtos: no máximo 90 (noventa) dias corridos a partir da emissão de Autorização de Fornecimento pelo IFSC; - Os equipamentos devem possuir atualização de firmware pelo período de garantia sem custos adicionais, sob responsabilidade da empresa licitante vencedora; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas. - Todos os equipamentos que necessitem de energia elétrica para seu funcionamento deverão vir acompanhados de cabos de alimentação conforme o padrão brasileiro NBR 14136 - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. | | | | |
| 15 | NOBREAK 3 KVA (Especificações mínimas): Características mínimas: - Potência:3000/3200 VA; - Frequência 50Hz/60Hz; - Bivolt automático: entrada 115/127V~ ou 220V~ e saída 115V~; - Fator de potência: 0,6; - Forma de onda senoidal pura; - Software para gerenciamento de energia; - Saída padrão USB ou RS-232 para comunicação inteligente (acompanha cabo USB tipo A-B); - Filtro de linha; - Estabilizador interno com 4 estágios de regulação; - Baterias seladas, internas e a prova de vazamentos; - True RMS; - Autoteste; - Autodiagnóstico; - Chave liga/desliga embutida no painel frontal que evita desligamento acidental; - Inversor sincronizado com a rede (sistema PLL); - LED indicador das condições do nobreak; - Alarme audiovisual: sinalização de eventos; - Permitir controlar e monitorar o nobreak via rede local (TCP/IP). - Proteções: Curto-circuito, sub/sobretensão, sobreaquecimento - Distorção harmônica (THD) com carga resistiva : <3%; - Rendimento : 85% (para operação bateria) - 08 tomadas padrão NBR 14136; - Gabinete deverá ser único, não sendo aceite montagens com o módulo de baterias sobreposto. - As baterias deverão estar dentro do gabinete formando um único equipamento (nobreak+baterias); - Não será aceito nobreaks cujas baterias fiquem fora do gabinete. - Garantia de 01 ano; - Garantia: 01 ano. | EQUIPAMENTO | 22 | 3.833,67 | 84.340,74 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 16 | NOBREAK 6 kVA Características mínimas: - Nobreak controlado por DSP (Processador Digital de Sinais); - Tecnologia online dupla conversão; - Correção de fator de potência ativo e unitário para carga linear ou carga não linear; - Forma de onda senoidal pura; - Autoteste; - LED indicador das condições do nobreak; - Função TRUE RMS; - Bypass automático e manual; - Distorção harmônica menor que 3% com carga linear; - Baterias seladas tipo VRLA internas e à prova de vazamento; - Recarga automática da bateria mesmo com o nobreak desligado garantindo maior tempo de vida útil; - Gerenciamento de bateria que avisa quando a bateria precisa ser substituída; - Equalização Automática da bateria a cada vez que o equipamento é ligado; - Estabilidade na frequência de saída; - Permitir utilização com grupo gerador - faixa de frequência na entrada (47Hz-63Hz); - Frequência de saída: 50/60Hz; - Chave liga/desliga embutida no painel frontal que evita desligamento acidental; - Ventilador interno controlado de acordo com o consumo de carga e da temperatura do nobreak; - Oito tomadas padrão NBR 14136 no próprio gabinte, não sendo permitido extesores; - Tensão de entrada nominal 110~220V (será definido no momento da compra); - Tensão de saída nominal 110~220V (será definido no momento da compra); - Comunicação serial padrão RS 232 ou USB; - Software de monitoração; - Interface SNMP RJ45; - Update de firmware; - Pot. nominal: 6000VA - Pot. contínua: 4800W - Fator de pot. Saída: 0,8 - Tensão nominal entrada: 110~220V - Freq. entrada: 47Hz - 63Hz - Fase: Monofásico - Conexão de entrada: Borneira - Tensão nominal saída: 110~220V - Fator de crista: 3:1 - Regulação dinâmica: <=3% - Regulação estática: <=1% - Tempo de transferência: 0 - Rend. pl. carga rede: 94% (dupla conversão) - Rend. pl. carga inversor: 94% (pela bateria) Autonomia - Típica: 18 min - Meia carga: 15 min - Plena carga: 7 min - Proteção: Sobrecarga, Curto-circuito, potência mínima, temperatura, bateria mínima; - Sinalização Sonora; - Gabinete: Metálico com tratamento anti-corrosivo e pintura epoxi; - Movimentação: Rodízios Giratórios; - As baterias deverão estar dentro do gabinete formando um único equipamento (nobreak+baterias); - Não será aceito nobreaks cujas baterias fiquem fora do gabinete. - Garantia de 01 ano; | EQUIPAMENTO | 26 | 11.369,14 | 295.597,64 |
| 17 | PONTO DE ACESSO INTERNO TIPO 1 --> Características técnicas mínimas: 1. A solução deverá ser composta de equipamentos do tipo thin access point, ou seja, APs que permitam acesso a rede ethernet via wireless, que possuam todas as suas configurações centralizadas na controladora Cisco modelo 5508 já instalada neste órgão. Os equipamentos deverão ser do mesmo fabricante da controladora acima citada por questões de operabilidade; 2. Hardware/unidade projetada com estrutura robusta, lacrada, sem espaços frontais para problemas com poeira e/ou umidade, com facilidades para fixação em parede ou teto, capaz de operar em ambiente de escritório. Deve acompanhar todos os acessórios para fixação em teto e/ou parede. Temperatura de operação de 5° a 40° C; 3. O AP deve suportar arquitetura centralizada onde o AP opera de modo dependente da controladora central WLAN que faz o gerenciamento das políticas de segurança, qualidade de serviço (QoS) e monitoramento de RF, utilizando para isto o protocolo de gerenciamento de RF específico; 4. As funcionalidades aqui descritas devem ser implementadas pelo conjunto ponto de acesso + controladora; 5. Implementar padrões IEEE 802.11A/B/G/N/AC simultaneamente com rádios distintos para 2.4 e 5 GHz, dentro do mesmo equipamento; 6. Suporte integrado a Power Over Ethernet (PoE) conforme o padrão IEEE 802.3af ou 802.3at; 7. Deve suportar, no mínimo, 16 (dezesseis) SSIDs com configurações distintas de rede, VLAN, segurança, criptografia e QoS; 8. Possuir 01(uma) interface Ethernet 10/100/1000 com conector RJ-45; 9. Deve possuir 01 (uma) interface de console, RJ-45, RS-232 ou USB, para gerenciamento completo local através de cabo console; 10. Deve possuir potência mínima de 150 mW em ambas as frequências. Não serão aceitos equipamentos com potência inferior; 11. Deve possuir LED frontal com intuito de obter-se status do equipamento; 12. Deve possibilitar implementação Plug-and-Play através de cliente DHCP, de modo que toda configuração seja baixada da controladora automaticamente; 13. Implementar gerenciamento automatizado de RF e potência, ou seja, os elementos da solução (Controlador + APs) devem definir sem intervenção manual os parâmetros de potência de transmissão e ajuste de canal de frequência, evitando interferências e sobreposição de canais; 14. Suporte a WMM; 15. Deve suportar operação MIMO 3x3 com sensibilidade mínima de -91 dBm operando em IEEE 802.11n (2.4GHz); 16. Deve possuir 3 antenas internas ao equipamento, operando como dual-band (transmissão e recepção simultânea nas duas faixas de frequência), com potência mínima de 4 dBi em 2.4 GHz e 4 dBi em 5 GHz. As antenas devem possuir radiação omnidirecional. Opcionalmente, pode ser fornecido equipamento com 6 antenas internas, 3 delas operando em 2.4 GHz e 3 delas operando em 5 GHz, com ganhos individuais de 4 dBi. Em ambas as formas o equipamento deverá operar com MIMO 3x3; 17. Deve operar com velocidades de até 867 Mbps e até 2 fluxos espaciais (spatial streams), de acordo com a disponibilidade de hardware do usuário; 18. Deve possuir funcionalidade para identificação de interferências nas frequências 2.4 e 5 GHz, com granularidade menor que 400 KHz, identificando | UNIDADE | 52 | 5.122,34 | 266.361,68 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | interferências provenientes de outros equipamentos que operem nas frequências relacionadas, como pontos de acesso, bluetooth, microondas, telefones sem fio e qualquer outro dispositivo que possua transmissão nestas faixas de frequências. Estas interferências devem ser classificadas e mitigadas pelo conjunto access point + controlador, quando possível. Esta análise deve ocorrer simultaneamente nas frequências 2.4 e 5 GHz no mesmo AP, sem qualquer interferência na transmissão de dados para os clientes conectados, ou seja, sem perda de conectividade ou redução de velocidade no acesso. No caso de não implementação desde recurso no mesmo equipamento, devem ser fornecidos dois pontos de acesso (desde que atendam aos requisitos deste item): um para operação de rede e outro para operação como análise de espectro; 19. Para segurança, o AP deve suportar os padrões IEEE 802.11i, WPA2, WPA, TLS, TTLS, MSCHAPv2, PEAP, EAP-FAST e EAP-SIM. O AP deve suportar TKIP para criptografia WPA e AES para criptografia WPA2; 20. Suportar autenticação segundo o padrão IEEE 802.1x com assinalamento de VLAN por usuário, conforme pré-definido em servidor Radius padrão de mercado (como por exemplo, FreeRadius e Microsoft IAS); 21. Possuir sistema anti-furto tipo Kensington Security Lock ou suporte específico para cadeado para proteção física do equipamento; 22. Deve estar homologado pela Anatel na data do pregão; 23. Deve vir totalmente habilitado e funcional para operação, sem restrição de licenças que habilitem funcionalidades específicas; 24. - A garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento, deverá ser pelo período mínimo de 36 meses; - A garantia deve incluir a reposição de equipamentos on site nos locais especificados neste termo de referência. - Os serviços serão solicitados mediante a abertura de um chamado, via chamada telefônica 0800, e-mail, website ou chat da licitante vencedora, e, constatada a necessidade, a mesma deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao IFSC; - O atendimento aos chamados deve ser realizado em até 1 dia útil a partir da abertura do chamado. - A resolução do problema e/ou defeito registrado deverá ocorrer, no máximo, em 15 dias corridos a partir da abertura do chamado. - Caso seja necessário a substituição do equipamento, a mesma deverá ser realizada em até 30 dias corridos, a partir da constatação pela equipe técnica da licitante vencedora, dentro do prazo de 15 dias conforme descrito no item anterior; - A licitante vencedora deve indicar, na assinatura da Ata de Registro de Preços, os procedimentos para abertura de suporte técnico; - A IFSC poderá solicitar o escalonamento de incidentes ao fabricante do equipamento quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware; - A garantia iniciará sua contagem a partir da data de emissão da NF dos equipamentos, serviços ou licenças. - Prazo de entrega de produtos: no máximo 90 (noventa) dias corridos a partir da emissão de Autorização de Fornecimento pelo IFSC; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, re-manufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas. - Todos os equipamentos que necessitem de energia elétrica para seu funcionamento deverão vir acompanhados de cabos de alimentação conforme o padrão brasileiro – NBR 14136; | | | | |
| 18 | PROJETOR DE IMAGENS PORTÁTIL – TIPO 1 Widescreen (Características mínimas): - Rede sem fio; - Método de projeção: Frontal / retroprojeção / preso ao teto; - Brilho em Cores: 3000 Lumens; - Brilho em Branco: 3000 Lumens; - Resolução: Widescreen HD (WXGA); - Relação de Contraste: 10.000:1; - Reprodução de cores: 16 milhões de cores; - Vida Útil da Lâmpada: mínimo 5000 horas (Modo Normal); - Entradas: HDMI x 1 \| VGA RGB : D-sub 15-pinos x 1 \| S-Vídeo: Mini DIN x 1 \| Vídeo Composto: RCA (Amarelo) x1 \| USB; - Entrada de Audio: RCA (Branco/Vermelho) x1; - Especificações Wireless: IEEE 802.11b: 11 Mbps, IEEE 802.11g: 54 Mbps, IEEE802.11n: 130 Mbps; - Tensão de alimentação: 100 - 240 V ±10%, 50/60 Hz; - Fornecer maleta ou sacola para transporte; - Orificio para cabo de segurança padrão Kensington. - Fornecer 1 cabo de segurança padrão Kensington com 2 chaves - Garantia 12 meses | EQUIPAMENTO | 96 | 4.505,00 | 432.480,00 |
| 19 | PROJETOR DE IMAGENS PORTÁTIL – TIPO 2(Características mínimas): - Rede sem fio; - Rede Ethernet RJ-45 x1; - Método de projeção: Frontal / retroprojeção / preso ao teto; - Brilho em Cores: 3000 Lumens; - Brilho em Branco: 3000 Lumens; - Resolução: (XGA); - Relação de Contraste: 10.000:1; - Reprodução de cores: 16 milhões de cores; - Vida Útil da Lâmpada: mínimo 5000 horas (Modo Normal); - Entrada para 2 computadores RGB; - Entradas: HDMI x 1 \| VGA RGB : D-sub 15-pinos x 2 \| S-Vídeo: Mini DIN x 1 \| Vídeo Composto: RCA (Amarelo) x1 \| USB A/B x1; - Entrada de Audio: RCA (Branco/Vermelho) x1; - Especificações Wireless: IEEE 802.11b: 11 Mbps, IEEE 802.11g: 54 Mbps, IEEE802.11n: 130 Mbps; - Tensão de alimentação: 100 - 240 V ±10%, 50/60 Hz; - Fornecer maleta ou sacola para transporte; - Orificio para cabo de segurança padrão Kensington. - Fornecer 1 cabo de segurança padrão Kensington com 2 chaves - Garantia 12 meses | EQUIPAMENTO | 83 | 2.350,00 | 195.050,00 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 20 | RACK DE PAREDE 19” x 09U; - 600mm de largura e profundidade de 600mm (mínimo) - Atender especificações ANSI/EIA RS-310-D, IEC 297-2; - Porta frontal reversível em vidro temperado, com fechadura tipo cilindro; - Confeccionado em aço SAE 1020; - Estrutura em aço 1.5 mm; - Capacidade de carga estática de 60kg; - Laterais com fecho rápido com a opção de utilização de chaves nas laterais; - Entrada e saída de cabos pelo teto ou pela base do rack com acabamento de proteção; - Teto com preparação para instalação de ventiladores; - Terminal de aterramento; - Deverá vir acompanhado: - Régua de tomadas 19” de 6 posições; - Um Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e; - Um guia de cabos; - Garantia mínima de 12 meses. | UNIDADE | 46 | 619,80 | 28.510,80 |
| 21 | RACK TORRE FECHADA 19" X 42U - Largura: 800 mm; - Altura: 42US; - Profundidade: 1000 mm; - Deve atender as especificações ANSI/EIA RS-310-E; - O equipamento deve ser totalmente desmontável para facilitar a montagem e o transporte (deverá ser entregue montado); - A estrutura deve ser em aço SAE 1010/1020 # 2 mm; - Deve possuir porta frontal curva em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°; - Deve possuir porta traseira bipartida em aço SAE 1010/1020 # 1,2 mm, com perfurações hexagonais (tipo colmeia), com índice de ventilação superior a 71% , com ângulo de abertura da porta de 180°; - Ambas as portas devem possuir fechaduras escamoteáveis com sistema automático de destrave; - Deve ser fornecido com tampas laterais em aço SAE 1010/1020 # 1,2 mm, removíveis através de fechos rápidos, com opção para colocação de fechadura; - O teto deve estar preparado para instalação de kit de ventiladores, tipo bandeja; - Deve possuir planos de montagem frontal e traseiro, galvanizados, anti-estáticos e numerados de 1 a 44 US; - Deve possuir2 guias de cabos verticais em aço SAE 1010/1020 # 1,0 mm, com anéis internos em termoplástico de alto impacto, nas dimensões de 44U x 95 mm x 70 mm (A x L x P), sendo fixadas na parte frontal do Rack; - O teto e a base do Rack deve ter abertura para entrada e saída de cabos, e tampas removíveis; - A estrutura do Rack deve possuir terminais de aterramento; - Deve ser fornecido com pés niveladores e rodízios, sendo 2 com travas e 2 sem travas; - Deve suportar uma carga estática até 800 kg; - O Rack deve possuir pintura micro epóxi na cor preta; - Deverá vir acompanhado: - Régua de tomadas 19” de 12 posições; - Três Patch Pannel 1U, com 24 portas com conectores fêmea RJ45 CAT 5e; - Três guia de cabos; - Garantia mínima de 12 meses. | UNIDADE | 6 | 4.879,43 | 29.276,58 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 22 | SERVIÇO DE INSTALAÇÃO FIREWALL TIPO 1 Especificações Mínimas: 1. Deverá ser prestado serviços de instalação e configuração, que compreendem, entre outros, os seguintes procedimentos: 1.1. Instalação física da solução incluindo ativação dos devidos licenciamentos e configurações de rede em camada 2 e camada 3 conforme solicitações da CONTRATANTE; 1.2. Configuração de filtro URL conforme solicitações da CONTRATANTE; 1.3. Atualização de sistema operacional e assinaturas de IPS; 1.4. Tunning de IPS para não haver bloqueios falso positivos das aplicações desenvolvidas internamente da CONTRATANTE; 1.5. Configuração da funcionalidade de controle de aplicações conforme solicitações da CONTRATANTE; 1.6. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas e boas práticas, cabendo a CONTRATANTE a aceitação ou não; 1.7. Num primeiro momento, todos os equipamentos devem ter suas configurações básicas, incluindo endereçamento IP, nome de usuário e senha local do usuário administrador, políticas de acesso e segurança, protocolo SNMP com autenticação e alta disponibilidade; 1.8. Devem ser realizados os mapeamentos necessários nos firewalls existentes, incluindo regras de acesso (ACL), NAT, PAT, nome e endereçamento das interfaces e o que for necessário para aplicação no novo equipamento; 1.9. O equipamento então deve ser configurado em bancada, atendendo as regras e configurações já existentes no ambiente. Sempre que possível, as regras devem ser melhoradas para aumento na segurança e facilidade de configuração e gerenciamento; 1.10. Em caso de necessidade de alteração da topologia da rede, é necessário o entendimento entre ambas as partes afim de reduzir o tempo de parada da rede; 1.11. A migração dos equipamentos deve ocorrer da forma mais transparente possível. Por isso o serviço deve ser realizado fora do horário comercial (entre 22:00 e 4:00). Caso o serviço não se reestabeleça até às 4:00, deve ser realizado o retorno para a solução antiga e posteriormente programada uma nova data para migração; 1.12. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência; 1.13. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes; 1.14. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas; 1.15. Após a instalação deve ser monitorado pelo prazo mínimo de 4 horas corridas as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação; 1.16. Ao final da instalação, deverá ser realizado o repasse de informações hands-on, apresentando as configurações realizadas nos equipamentos, de no mínimo 2 (duas) horas, ou conforme disposto individualmente em cada item (prevalecendo o disposto individualmente em cada item). A CONTRATANTE disponibilizará o local adequado para a transferência do conhecimento e acesso aos equipamentos de produção; 1.17. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a CONTRATANTE poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas; 1.18. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços; 1.19. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE. | SERVIÇO | 1 | 26.543,68 | 26.543,68 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 23 | SERVIÇO DE INSTALAÇÃO FIREWALL TIPO 2 Especificações Mínimas: 1. Deverá ser prestado serviços de instalação e configuração, que compreendem, entre outros, os seguintes procedimentos: 1.1. Instalação física da solução incluindo ativação dos devidos licenciamentos e configurações de rede em camada 2 e camada 3 conforme solicitações da CONTRATANTE; 1.2. Configuração de filtro URL conforme solicitações da CONTRATANTE; 1.3. Atualização de sistema operacional e assinaturas de IPS; 1.4. Tunning de IPS para não haver bloqueios falso positivos das aplicações desenvolvidas internamente da CONTRATANTE; 1.5. Configuração da funcionalidade de controle de aplicações conforme solicitações da CONTRATANTE; 1.6. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas e boas práticas, cabendo a CONTRATANTE a aceitação ou não; 1.7. Num primeiro momento, todos os equipamentos devem ter suas configurações básicas, incluindo endereçamento IP, nome de usuário e senha local do usuário administrador, políticas de acesso e segurança, protocolo SNMP com autenticação e alta disponibilidade; 1.8. Devem ser realizados os mapeamentos necessários nos firewalls existentes, incluindo regras de acesso (ACL), NAT, PAT, nome e endereçamento das interfaces e o que for necessário para aplicação no novo equipamento; 1.9. O equipamento então deve ser configurado em bancada, atendendo as regras e configurações já existentes no ambiente. Sempre que possível, as regras devem ser melhoradas para aumento na segurança e facilidade de configuração e gerenciamento; 1.10. Em caso de necessidade de alteração da topologia da rede, é necessário o entendimento entre ambas as partes afim de reduzir o tempo de parada da rede; 1.11. A migração dos equipamentos deve ocorrer da forma mais transparente possível. Por isso o serviço deve ser realizado fora do horário comercial (entre 22:00 e 4:00). Caso o serviço não se reestabeleça até às 4:00, deve ser realizado o retorno para a solução antiga e posteriormente programada uma nova data para migração; 1.12. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência; 1.13. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes; 1.14. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas; 1.15. Após a instalação deve ser monitorado pelo prazo mínimo de 4 horas corridas as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação; 1.16. Ao final da instalação, deverá ser realizado o repasse de informações hands-on, apresentando as configurações realizadas nos equipamentos, de no mínimo 2 (duas) horas, ou conforme disposto individualmente em cada item (prevalecendo o disposto individualmente em cada item). A CONTRATANTE disponibilizará o local adequado para a transferência do conhecimento e acesso aos equipamentos de produção; 1.17. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a CONTRATANTE poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas; 1.18. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços; 1.19. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE. | SERVIÇO | 4 | 6.713,52 | 26.854,08 |
| 24 | SERVIDOR DE RACK Especificações mínimas: 1 - Deverá estar na atual linha de produção do fabricante; 2 - Gabinete tipo Rack original do fabricante do equipamento, com tamanho de 1U; 3 - 01 (hum) Processador de 8 (oito) núcleos, de pelo menos 1.7 GHz, 85 Watts de | EQUIPAMENTO | 18 | 24.689,00 | 444.402,00 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | consumo, 20MB cache, expansível a 22 (vinte e dois) núcleos com a instalação de um segundo processador (expansão para 2 processadores), compatível com instruções de 32 bits no padrão x86 e 64 bits, do segmento de servidores; 4 - BIOS desenvolvida pelo próprio fabricante do equipamento, não sendo aceito regime OEM ou adaptações feitas através de direitos copyrights; 5 - Memória de 32GB DDR4-2400, com recursos advanced ECC, homologada pelo próprio fabricante; expansível a, pelo menos, 1,5TB; 6 - Controladora de disco com suporte a RAID 0, 1, 10 e 5; 7 - Possuir no mínimo 06 (seis) unidades de disco NearLine SATA de 1,6 TB cada, totalizando 9,6 TB. Unidades de disco padrão HOT PLUG, configurados em modo RAID 5 compatíveis com a controladora RAID ofertada; 8 - Possuir display ou led de diagnostico acoplado no servidor para alertar e monitorar as condições de funcionamento do equipamento; 9 - Possuir no mimino 1 slot PCI-Express x8 para expansão e 1 slot PCI-Express x16 para expansão; 10 - Possui 01 (uma) unidade optica DVD-ROM para leitura de CD e DVD no mesmo padrão de cor e tonalidade do gabinete; 11 - Interface Controladora de vídeo Padrão VGA; 12 - Controladora de rede com quatro (4) portas, conector RJ-45; 13 - Interfaces de rede padrão Gigabit Ethernet com suporte à tecnologia TSO (TCP segmentation offload) ou TOE (TCP/IP Offload Engine); Operar automaticamente nas velocidades de comunicação de 10/100/1000Mbps, bem como no modo full-duplex; Compatibilidade funcional e operacional com os padroes IEEE 802.3 para 10baseT (Ethernet), IEEE 802.3u para 100baseTX (Fast Ethernet) e IEEE 802.3ab para 1000baseT (Gigabit Ethernet); Possui recursos de Wake on LAN (WOL);Suporta boot através de protocolo PXE; Suporta Virtual LANs, Jumbo Frames, Link aggregation e Load Balancing; 14 - Gabinete tipo rack com ventilação otimizada para tal configuração; Kit de trilhos e braço organizador de cabos para fixação dos equipamentos em rack padrão 19 polegadas, permitindo o deslizamento do equipamento a fim de facilitar a manutenção; Gabinete tipo "tool less" (abertura do gabinete sem a utilização de ferramentas); 15 - Fontes de alimentação redundantes, HOT PLUG, para funcionamento em 110 ou 240Vac com potência suficiente para suportar a máxima configuração do equipamento, acompanhado de 02 cabos de alimentação padrão NBR14136; 16 - A solução deverá suportar Trusted Platform Module (TPM) 2.0 usado para gerar, armazenar chaves, Proteger, autenticar senhas e criar e armazenar certificados digitais. 17 - Deverá ser fornecido solução de software de gerenciamento, desenvolvido pelo mesmo fabricante do servidor compatível com o padrão IPMI 2.0 ou SNMP e suportar os seguintes recursos: a) Permite o gerenciamento centralizado dos servidores através de interface WEB; b) Realiza inventario de hardware, BIOS, firmware e drivers e armazena-lo em repositório de forma a possibilitar relatórios customizados; c) Possui recurso de update de BIOS, Firmware e Drivers; d) Permite o monitoramento de performance e consumo de energia dos servidores; e) Emite alertas de falha de hardware e permite a criação de filtros de alertas isolados e notificação por e-mail; f ) Suporte aos padrões SNMP, DMI e IPMI; h) Possuir recurso de mídia e kvm virtual; g) Compatibilidade com os sistemas operacionais Windows, Linux; 05 (cinco) anos de atualização gratuita para o software de administração/gerenciamento; 18 - Fornecer documentos que comprovem que o equipamento (modelo) consta na HCL da Microsoft para o Windows 2012 Server ou superior e na HCL da Red Hat 6 para o Enterprise Server 6.0 ou superior (obtido no site da Microsoft e Red Hat. Será aceito a impressão das páginas que atestam isso); 19 - Deverá ser entregue Certificado ou Relatório de Avaliação de Conformidade emitido por um órgão credenciado pelo INMETRO ou Certificado similar ou, ainda, comprovação mediante apresentação em catalogo do fabricante, de que o equipamento está em conformidade com a norma IEC 60950 (Safety of Information Technology Equipment Including Eletrical Business Equipment), para segu-rança do usuario contra incidentes elétricos e combustão dos materiais elétricos; 20 - Deverá ser fornecido declaração da licitante informando que o equipamento não contem subs-tancias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cadmio (Cd), bifenil polibromados (PBBs), eteres difenilpolibromados (PBDEs) em concentração acima da re-comendada na diretiva RoHS (Restriction of Certain Hazardous Substances). 21 - Todas as características descritas devem ser comprovadas através de catálogos, manuais, etc; 22 - Garantia de 5 anos com atendimento no próximo dia util. Os produtos fornecidos estarão cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento; 23 - Declaração da licitante informando a rede autorizada de assistência técnica no Estado de Santa Catarina. Durante o período de garantia a empresa vencedora devera, sem ônus adicional, fornecer as atualizações ("patches") corretivas do software e firmware do equipamento fornecido; A empresa vencedora prestará garantia ao sistema fornecido nas seguintes condições: fornecerá informações detalhadas sobre o suporte técnico gratuito (inclusive a ligação telefônica por meio de DDG) em português durante o período de garantia, incluindo atualização de software. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada gratuita (DDG) em horário comercial, de | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | segunda a sexta-feira (8x5). A contratada deverá possuir central de atendimento técnico, com abertura de chamados via DDG 0800 realizando a gestão dos processos de suporte e atendimento ‘’on-site”. O equipamento deverá possuir 5 anos de garantia “on-site” com atendimento 24 horas, 7 dias por semana com presença de um técnico “on-site” no próximo dia útil; Os componentes, peças e materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento; 24 - Condições de Entrega: O transporte dos equipamentos até o local especificado, será realizado pela empresa vencedora (inclusive os procedimentos de seguro, embalagem e transporte até o local especificado); A verificação quanto ao estado dos equipamentos após o transporte será de exclusiva responsabilidade da empresa vencedora, sendo que, quaisquer danos observados no transporte, a qualquer tempo, serão reparados pela empresa vencedora. 25 – Serviço de Instalação: A instalação dos equipamentos será feita no local indicado pela contratante, por profissionais devidamente qualificados e certificados pelo fabricante; A instalação compreende o que segue: – Instalação física: Após o aceite do equipamento a empresa vencedora devera agendar com um técnico do IFSC dia e hora da instalação, que deverá ser feita em armário (rack) próprio, disponibilizado pela contratante; – O técnico da empresa vencedora deverá expor para o técnico do IFSC as tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados; – A empresa vencedora emitirá declaração da realização da instalação, em papel timbrado, constando hora, data e local da realização desta atividade. Neste documento constará, também, o nome do técnico da empresa vencedora que realizou a demonstração e os nomes dos técnicos do IFSC que participaram, com a assinatura de todos. 26 - Condições Gerais de Fornecimento: Todos os itens de Hardware deverão ser do mesmo fabricante, mesmo que em regime OEM, neste ultimo caso apresentar comprovação desta condição; O sistema deverá ser fornecido com todos os cabos necessários para a interconexão dos equipamentos adquiridos, além de todos os acessórios de montagem e operação; A solução somente será considerada devidamente entregue após a sua completa instalação e a realização de testes, devendo o sistema estar em perfeitas condições de funcionamento; Apresentar atestado de capacidade técnica compatível com os equipamentos solicitados em quantidade similar com fornecimento e instalação; Deverá ser apresentada declaração de revenda autorizada; Os serviços constantes deverão ser executados por profissionais com no mínimo as seguintes certificações onde se aplicam: 01 Profissional com certificação oficial do fabricante para integração de servidores. Comprovação através da apresentação do certificado. Os serviços de manutenção e suporte deverão ser prestados pelo próprio fabricante do equipamento ou através da proponente; A instalação de todos os itens deve prever uma janela de manutenção estabelecida entre o IFSC e o licitante; Instalação física, cabeamento e conectorização dos equipamentos, ao ambiente atual da IFSC; Os serviços descritos deverão ser executados em horário comercial; - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a “repetição” deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. | | | | |
| 25 | SERVIDOR TIPO BLADE - Características: Deverá estar na atual linha de produção do fabricante; Deverá ser totalmente compatível com o modelo de Chassis HP BLc7000 existentes no IFSC; 02 (dois) Processadores de 12 (doze) núcleos, de pelo menos 2.2 GHz, 105 Watts de consumo, 30MB cache, compatível com instruções de 32 bits no padrão x86 e 64 bits; BIOS é desenvolvida pelo fabricante do equipamento ou o fabricante possui direitos de copyright sobre a BIOS. Será aceito soluções em regime de OEM; Memória de 256GB DDR4-2400, com recursos advanced ECC, homologada pelo próprio fabricante; expansível a, pelo menos, 512GB; Controladora de discos SAS com suporte a RAID 0, 1; Possuir 02 (duas) unidades de disco SAS de 300GB cada. Unidades de disco padrão HOT PLUG, configurados em modo RAID 1 compatíveis com a controladora RAID ofertada; Possuir 2 mezzanine slots; Duas portas de rede convergentes 10 Gigabit Ethernet disponíveis para o servidor. Suporte aos protocolos padrão IEEE 802.1p QoS, 802.1Q VLAN tagging, 802.3ad link aggregation, 802.3ap 10GBase-KR e 802.3x flow control, com modo de operação 1000 Mbps e 10.000 Mbps Full Duplex. Possuir placa mezzanine com 2 portas FC, com as velocidades full-duplex de 8Gbps de forma auto negociada; Gabinete tipo “tool less” (abertura do gabinete sem a utilização de ferramentas); A solução deverá suportar Trusted Platform Module (TPM) 2.0 usado para gerar, armazenar chaves, Proteger, autenticar senhas e criar e armazenar certificados digitais. Deverá ser fornecido documentos que comprovem que o equipamento (modelo) | UNIDADE | 3 | 61.267,64 | 183.802,92 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | consta na HCL da Mi-crosoft para o Windows 2012 Server ou superior e na HCL da Red Hat 6 para o Enterprise Server 6.0 ou superior (obtido no site da Microsoft e Red Hat. Será aceito a impressão das páginas que atestam isso); Deverá ser fornecido declaração da licitante informando que o equipamento não contem substancias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cadmio (Cd), bifenil polibromados (PBBs), eteres difenilpolibromados (PBDEs) em concentração acima da re-comendada na diretiva RoHS (Restriction of Certain Hazardous Substances). Garantia de 5 anos com tempo de solução de 6 horas no formato 24x7. Os produtos fornecidos estarão cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento; Declaração da licitante informando a rede autorizada de assistência técnica no Estado de Santa Catarina. Durante o período de garantia a empresa vencedora devera, sem ônus adicional, fornecer as atualizações (“patches”) corretivas do software e firmware do equipamento fornecido; A empresa vencedora prestará garantia ao sistema fornecido nas seguintes condições: fornecerá informações detalhadas sobre o suporte técnico gratuito (inclusive a ligação telefônica por meio de DDG) em português durante o período de garantia, incluindo atualização de software. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada gratuita (DDG) em horário comercial, de segunda a sexta-feira (24x7); Os componentes, peças e materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento; Condições de Entrega: O transporte dos equipamentos até o local especificado, será realizado pela empresa vencedora (inclusive os procedimentos de seguro, embalagem e transporte até o local especificado); A verificação quanto ao estado dos equipamentos após o transporte será de exclusiva responsabilidade da empresa vencedora, sendo que, quaisquer danos observados no transporte, a qualquer tempo, serão reparados pela empresa vencedora. Serviço de Instalação: A instalação dos equipamentos será feita no local indicado pela contratante, por profissionais devidamente qualificados e certificados pelo fabricante; A instalação compreende o que segue: – Instalação física: Após o aceite do equipamento a empresa vencedora devera agendar com um técnico do IFSC dia e hora da instalação, que deverá ser feita em armário (rack) próprio, disponibilizado pela contratante; – O técnico da empresa vencedora deverá expor para o técnico do IFSC as tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados; – A empresa vencedora emitirá declaração da realização da instalação, em papel timbrado, constando hora, data e local da realização desta atividade. Neste documento constará, também, o nome do técnico da empresa vencedora que realizou a demonstração e os nomes dos técnicos do IFSC que participaram, com a assinatura de todos. Apresentação de, no mínimo, um Atestado de Capacidade Técnica, emitido por pessoa jurídica de direito público ou privado, comprovando que o Licitante fornece/forneceu bens compatível com o objeto da licitação (computador servidor em lâmina), emitido em papel timbrado com assinatura, identificação e telefone do emitente; Os serviços constantes deverão ser executados por profissionais com no mínimo as seguintes certificações onde se aplicam:01 Profissional com certificação oficial do fabricante para integração de servidores; Os serviços de manutenção e suporte deverão ser prestados pelo próprio fabricante do equipamento; A instalação de todos os itens deve prever uma janela de manutenção estabelecida entre o IFSC e o licitante; Instalação física, cabeamento e conectorização dos equipamentos ao ambiente atual da IFSC; Os serviços descritos deverão ser executados em horário comercial; | | | | |
| 26 | SOFTWARE TABLEAU Licenças perpétua com suporte e manutenção por 12 meses do Software Tableau Desktop Professional que permita ao usuário a exploração e análise de dados, além da criação, atualização e visualização de número ilimitado de gráficos, relatórios, painéis de informações gerenciais e histórias de dados de informações gerenciais OU licença similar de tipo ou qualidade superior ao Tableau Desktop Professional. | LICENÇA | 1 | 7.179,41 | 7.179,41 |
| 27 | SWITCH 24 PORTAS GIGABIT L2 Distribuição 1. Equipamento tipo switch gigabit ethernet com capacidade de operação em camada 2 do modelo OSI; 2. Deve ser fornecido com 24 (vinte e quatro) portas 100/1000BaseT, conector RJ-45; 3. Deve ser fornecido com 4 slots SFP para conexão de transceivers SFP com fibras ópticas multimodo e monomodo. Estas portas não devem ser do tipo COMBO com as portas do item anterior; 4. Deve possuir 28 portas ativas simultaneamente; 5. Deve possuir porta de console USB e Ethernet (RJ-45) para gerenciamento local; 6. Deve possuir capacidade de vazão de pelo menos 71 mpps; 7. Deve permitir o espelhamento do tráfego de uma porta (port mirroring) para outra porta o mesmo switch; 8. Deve possuir Jumbo Frame de 9000 bytes; 9. Deve possuir IGMP para tráfego de multicast; 10. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, e deve permitir a criação de no mínimo 1023 VLANs com IDs entre 1 e 4096; 11. Deve identificar automaticamente portas | EQUIPAMENTO | 76 | 14.165,52 | 1.076.579,52 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | em que telefones IP estejam conectados e associá-las automaticamente a VLAN de voz; 12. Deve possuir autenticação IEEE 802.1x com assinalamento de VLAN por usuário e Guest VLAN para usuários não autenticados; 13. Deve permitir configurar quantos endereços MAC podem ser aprendidos em uma porta (port security); 14. Deve implementar access control list com suporte a 512 regras; 15. Deve ser possível filtrar pacotes usando endereço IP, endereço MAC, porta, campo DSCP, prioridade 802.1p; 16. Deve aplicar controle de banda (rate limit) usando para isso regras de ACL; 17. Deve possuir funcionalidade para supressão de tráfego broadcast, multicast e unicast unknown; 18. Deve possuir Spanning Tree padrão IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree) com filtros BPDU; 19. Deve possuir o protocolo SNTP ou NTP para a sincronização do relógio com outros dispositivos; 20. Deve possuir priorização de pacotes (QoS) com 4 filas de prioridade por porta; 21. Deve possuir cliente DNS; 22. Deve implementar IPv6 incluindo endereçamento IP, ICMP e operação dual-stack. Além disso, deve implementar IPv6 QoS em hardware; 23. Deve permitir a configuração de DHCP Relay; 24. Deve permitir configuração/administração remota através de interface gráfica web-based SSL, SSH, SNMP e TFTP; 25. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1AB para descobrimento de uplinks; 26. Deve permitir o envio de mensagens geradas pelo sistema em servidor externo (syslog); 27. Deve permitir o Empilhamento através da adição de módulo e cabo adicional (não inclusos). O módulo de portas de empilhamento e o cabo não precisam ser fornecidos neste processo; 28. Deve possuir largura de banda para empilhamento no mínimo de 80G, quando adicionado o módulo adicional; 29. Deve permitir a agregação de segmentos ethernet paralelos em uma única interface, possibilitando aumento da largura de banda e redundância; 30. Deve ser fornecido cabo console RJ45 original com no mínimo 1,5m; 31. Deve atender aos seguintes padrões IEEE: - IEEE 802.1D Spanning Tree Protocol - IEEE 802.1p CoS Prioritization - IEEE 802.1Q VLAN - IEEE 802.1s - IEEE 802.1w - IEEE 802.1X - IEEE 802.1ab (LLDP) - IEEE 802.3ad - IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports - IEEE 802.3 10BASE-T - IEEE 802.3u 100BASE-TX - IEEE 802.3ab 1000BASE-T - IEEE 802.3z 1000BASE-X - RMON I and II standards - SNMP v1, v2c, and v3 - IEEE 802.3az - IEEE 802.3ae 10Gigabit Ethernet - IEEE 802.1ax 32. Deve atender aos seguintes padrões RFC: - RFC 768 - UDP - RFC 783 - TFTP - RFC 791 - IP - RFC 792 - ICMP - RFC 793 - TCP - RFC 826 - ARP - RFC 854 - Telnet - RFC 951 - Bootstrap Protocol (BOOTP) - RFC 959 - FTP - RFC 1112 - IP Multicast and IGMP - RFC 1157 - SNMP v1 - RFC 1166 - IP Addresses - RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery - RFC 1305 - NTP - RFC 1492 - TACACS+ - RFC 1493 - Bridge MIB - RFC 1542 - BOOTP extensions - RFC 1643 - Ethernet Interface MIB - RFC 1757 - RMON - RFC 1901 - SNMP v2C - RFC 1902-1907 - SNMP v2 - RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6 - FRC 2068 - HTTP - RFC 2131 - DHCP - RFC 2233 - IF MIB v3 - RFC 2460 - IPv6 - RFC 2461 - IPv6 Neighbor Discovery - RFC 2462 - IPv6 Autoconfiguration - RFC 2463 - ICMP IPv6 - RFC 2474 - Differentiated Services (DiffServ) Precedence - RFC 2597 - Assured Forwarding - RFC 3046 - DHCP Relay Agent Information Option - RFC 3580 - 802.1X RADIUS 33. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática; 34. Gabinete padrão para montagem em rack de 19", incluindo todos os acessórios; 35. O equipamento deve possuir garantia pelo período de 36 (trinta e seis) meses com envio de peças de reposição em até 3 dias úteis; - A garantia deve incluir o envio de equipamentos de reposição que deverão ser entregues nos locais especificados neste termo de referência. - Os serviços serão solicitados mediante a abertura de um chamado, via chamada telefônica 0800, e-mail, website ou chat da licitante vencedora, e, constatada a necessidade, a mesma deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante; - O atendimento aos chamados deve ser realizado em até um dia útil a partir da abertura do chamado. - A resolução do problema e/ou defeito registrado deverá ocorrer, no máximo, em 15 dias corridos a partir da abertura do chamado. - Caso seja necessário a substituição do equipamento, a mesma deverá ser realizada em até 30 dias corridos, a partir da constatação pela equipe técnica da licitante vencedora, dentro do prazo de 15 dias conforme descrito no item anterior; - A licitante vencedora deve indicar, na assinatura da Ata de Registro de Preços, os procedimentos para abertura de suporte técnico; - A licitante vencedora deve possuir, no momento da assinatura da Ata de Registro de Preços, pelo menos 1 (um) profissional com certificação técnica específica da tecnologia empregada (SWITCH) emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; Comprovação através da apresentação da certificação. - A contratante poderá solicitar o escalonamento de incidentes ao fabricante do equipamento quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware; - A garantia iniciará sua contagem a partir da data de | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | emissão da NF dos equipamentos, serviços ou licenças. - Prazo de entrega de produtos: no máximo 90 (noventa) dias corridos a partir da emissão de Autorização de Fornecimento pelo IFSC; - Os equipamentos devem possuir atualização de firmware pelo período de garantia sem custos adicionais, sob responsabilidade da empresa licitante vencedora; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas, não sendo aceitos equipamentos com caixas violadas. - Todos os equipamentos que necessitem de energia elétrica para seu funcionamento deverão vir acompanhados de cabos de alimentação conforme o padrão brasileiro – NBR 14136. - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. | | | | |
| 28 | SWITCH 24 PORTAS GIGABIT L2 Acesso 1. Equipamento tipo switch gigabit ethernet com capacidade de operação em camada 2 do modelo OSI; 2. Deve ser fornecido com 24 (vinte e quatro) portas 100/1000BaseT, conector RJ-45; 3. Deve ser fornecido com 2 slots SFP para conexão de transceivers SFP com fibras ópticas multimodo e monomodo. Estas portas não devem ser do tipo COMBO com as portas do item anterior; 4. Deve ser fornecido com 2 portas 100/1000BaseT e conector RJ-45 adicionais para uplink com outros equipamentos; 5. Deve possuir 26 portas ativas simultaneamente; 6. Deve possuir porta de console para gerenciamento local; 7. Deve possuir capacidade de vazão de pelo menos 38 mpps; 8. Deve permitir o espelhamento do tráfego de uma porta (port mirroring) para outra porta do mesmo switch; 9. Deve possuir Jumbo Frame de 9000 bytes; 10. Deve possuir IGMP para tráfego de multicast; 11. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, e deve permitir a criação de no mínimo 64 VLANs com IDs entre 1 e 4094; 12. Deve identificar automaticamente portas em que telefones IP estejam conectados e associá-las automaticamente a VLAN de voz; 13. Deve possuir autenticação IEEE 802.1x com assinalamento de VLAN por usuário e Guest VLAN para usuários não autenticados; 14. Deve permitir configurar quantos endereços MAC podem ser aprendidos em uma porta (port security); 15. Deve implementar access control list com suporte no mínimo a 512 regras; 16. Deve ser possível filtrar pacotes usando endereço IP, endereço MAC, porta, campo DSCP, prioridade 802.1p; 17. Deve aplicar controle de banda (rate limit) usando para isso regras de ACL; 18. Deve possuir funcionalidade para supressão de tráfego broadcast, multicast e unicast unknown; 19. Deve possuir Spanning Tree padrão IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree) com filtros BPDU; 20. Deve possuir o protocolo SNTP ou NTP para a sincronização do relógio com outros dispositivos; 21. Deve possuir priorização de pacotes (QoS) com 4 filas de prioridade por porta; 22. Deve possuir cliente DNS; 23. Deve implementar IPv6 incluindo endereçamento IP, ICMP e operação dual-stack. Além disso, deve implementar IPv6 QoS em hardware; 24. Deve permitir a configuração de DHCP Relay; 25. Deve permitir configuração/administração remota através de interface gráfica web-based SSL, SSH, SNMP e TFTP; 26. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1AB para descobrimento de uplinks; 27. Deve permitir o envio de mensagens geradas pelo sistema em servidor externo (syslog); 29. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática; 30. Gabinete padrão para montagem em rack de 19", incluindo todos os acessórios; 31. Deve atender aos seguintes padrões IEEE e RFC: IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w RSTP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1350, RFC 1533, RFC 1541, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC2576, RFC 4330, RFC 1213, RFC 1215, RFC 1286, RFC 1442, RFC 1451, RFC 1493, RFC 1573, RFC 1643, RFC 1757, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2233, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 1157, RFC 1493, RFC 1215, RFC 3416 32. Deve atender as seguintes RFCs para IPV6. RFC 4443 (which obsoletes RFC2463) - ICMP version 6, RFC 4291 (which obsoletes RFC | EQUIPAMENTO | 112 | 3.958,51 | 443.353,12 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | 3513) - IPv6 address architecture, RFC 4291 - IPv6 addressing architecture, RFC 2460 - IPv6 specification, RFC 4861 (which obsoletes RFC 2461) - Neighbor discovery for IPv6, RFC 4862 (which obsoletes RFC 2462) - IPv6 stateless address auto-configuration, RFC 1981 - Path MTU discovery, RFC 4007 - IPv6 scoped address architecture, RFC 3484 - Default address selection mechanism; 33. Deve ser fornecido cabo console RJ45 original com no mínimo 1,5m; 34. O equipamento deve possuir garantia pelo período de 36 (trinta e seis) meses com envio de peças de reposição em até 3 dias úteis; - A garantia deve incluir o envio de equipamentos de reposição que deverão ser entregues nos locais especificados neste termo de referência. - Os serviços serão solicitados mediante a abertura de um chamado, via chamada telefônica 0800, e-mail, website ou chat da licitante vencedora, e, constatada a necessidade, a mesma deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante; - O atendimento aos chamados deve ser realizado em até um dia útil a partir da abertura do chamado. - A resolução do problema e/ou defeito registrado deverá ocorrer, no máximo, em 15 dias corridos a partir da abertura do chamado. - Caso seja necessário a substituição do equipamento, a mesma deverá ser realizada em até 30 dias corridos, a partir da constatação pela equipe técnica da licitante vencedora, dentro do prazo de 15 dias conforme descrito no item anterior; - A licitante vencedora deve indicar, na assinatura da Ata de Registro de Preços, os procedimentos para abertura de suporte técnico; A licitante vencedora deve possuir, no momento da assinatura da Ata de Registro de Preços, pelo menos 1 (um) profissional com certificação técnica específica da tecnologia empregada (SWITCH) emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; Comprovação através da apresentação da certificação. - A contratante poderá solicitar o escalonamento de incidentes ao fabricante do equipamento quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware; - A garantia iniciará sua contagem a partir da data de emissão da NF dos equipamentos, serviços ou licenças. - Prazo de entrega de produtos: no máximo 90 (noventa) dias corridos a partir da emissão de Autorização de Fornecimento pelo IFSC; - Os equipamentos devem possuir atualização de firmware pelo período de garantia sem custos adicionais, sob responsabilidade da empresa licitante vencedora; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas, não sendo aceitos equipamentos com caixas violadas. - Todos os equipamentos que necessitem de energia elétrica para seu funcionamento deverão vir acompanhados de cabos de alimentação conforme o padrão brasileiro – NBR 14136. - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. | | | | |
| 29 | Item: SWITCH 24 PORTAS PoE GIGABIT DISTRIBUIÇÃO Especificações Mínimas: 1. Comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve ser fornecido com 24 (vinte e quatro) portas 100/1000BaseT, conectores RJ-45 fornecido diretamente no equipamento; 3. Deve prover alimentação PoE+ conforme o padrão IEEE 802.3at nas 24 (vinte e quatro) portas 100/1000 BaseT, com 370W exclusivos para alimentação PoE, a serem alocados em todas as portas. Não serão aceitas fontes externas ou módulos adicionais para alimentação PoE; 4. Deve ser fornecido com 4 slots SFP para conexão de transceivers SFP para fibras ópticas multimodo e monomodo. Estas portas devem ser de uso simultâneo com as portas do item anterior e não serão aceitas interfaces do tipo combo; 5. Deve possuir 28 portas ethernet ativas simultaneamente, não incluindo interfaces de empilhamento; 6. Deve possuir capacidade de vazão de pelo menos 70 mpps, com switching bandwidth de 116 Gbps Full-duplex; 7. Deve suportar empilhamento através de interfaces dedicadas, com velocidade mínima de 64 Gbps Full duplex na pilha, configurado em forma de anel, formando pilhas de pelo menos 8 unidades. Deve-se utilizar portas específicas para este fim, de uso traseiro. Caso seja opcional, a porta e cabo de empilhamento não precisam ser fornecidos neste processo. Deve empilhar com switches PoE e não PoE. Os switches PoE devem prover alimentação conforme o padrão 802.3at, fornecendo até 30W por porta. Deve permitir a criação de links agrupados virtualmente (link aggregation) utilizando portas de diferentes switches da pilha; 8. Deve possuir porta de console frontal para total gerenciamento local, com conector RS-232, RJ-45 ou USB; 9. O equipamento deve permitir sua configuração automática com base em outro equipamento da rede, sem intervenção humana, permitindo a | EQUIPAMENTO | 36 | 21.299,00 | 766.764,00 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | rápida substituição do equipamento. Ao ser ligado, o equipamento deve buscar esta configuração em outro equipamento da rede, utilizando-se para isso parâmetros fornecidos pelo DHCP; 10. Deve possuir Jumbo Frame de pelo menos 9000 bytes; 11. Deve ser fornecido com capacidade instalada para operar em conformidade com o padrão IEEE 802.1Q para criação de redes virtuais, e deve permitir a criação de no mínimo 512 VLANs com 4096 VLAN ID; 12. O equipamento deve suporta a criação de 8 rotas estáticas para criação de pequenos backbones; 13. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring); 14. Deve permitir a criação de links agrupados virtualmente (link aggregation); 15. Deve possuir funcionalidade de LLDP conforme o padrão IEEE 802.1ab, que permita o autodescobrimento do equipamento conectado na porta do switch. A detecção do equipamento conectado deve ocorrer de forma automática; 16. Deve possuir IGMP snooping com pelo menos 256 grupos para controle de tráfego de multicast; 17. Deve identificar automaticamente portas em que telefones IP estejam conectados e associá-las automaticamente a VLAN de voz; 18. Deve possuir Spanning Tree padrão IEEE 802.1w (Rapid Spanning Tree), IEEE 802.1s (Multiple Spanning Tree) com filtros BPDU e spanning tree por vlan. Deve implementar pelo menos 32 instâncias; 19. Deve possuir priorização de pacotes (QoS) com 4 filas de prioridade por porta. Deve implementar a classificação de pacotes com base em regras de ACL; 20. Deve possuir autenticação IEEE 802.1x com assinalamento de VLAN por usuário e Guest VLAN para usuários não autenticados. Para usuários sem cliente IEEE 802.1x instalado, deve possuir um portal Web interno ao equipamento para autenticação; 21. Deve possuir autenticação IEEE 802.1x de múltiplos usuários por porta, para o caso de links com switches não gerenciáveis. Apenas o tráfego dos usuários que se autenticarem será permitido; 22. Deve implementar criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes a senha; 23. Deve permitir configurar quantos endereços MAC podem ser aprendidos em uma porta, e permitir configurar qual ação será tomada quando esta regra for quebrada; 24. Deve permitir a criação de listas de acesso (ACLs) em IPv4, internamente ao equipamento, baseadas em endereço IP de origem, endereço IP de destino, protocolo, portas TCP, UDP, ICMP, IGMP, campo DSCP, campo ToS e dia e hora. Deve ser possível definir ACL por VLAN e habilitar o log da ACL; 25. Deve implementar IPv6 com as seguintes RFCs: 1981, 2373, 2460, 2461, 2462 e 2463; 26. Deve permitir a configuração de DHCP Server e DHCP Relay com suporte a múltiplas VLANs simultaneamente; 27. Deve possuir DHCP Snooping para eliminação de falsos servidores de DHCP; 28. Deve possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC, de forma a evitar ataques na rede; 29. Deve responder a pacotes para teste de rede, suportando no mínimo as seguintes operações de teste: TCP connect e UDP echo. Caso o equipamento ofertado não forneça essa funcionalidade, deve ser fornecida ferramenta capaz de prover estas funcionalidades; 30. Deve possuir o protocolo "Network Time Protocol" (NTP), autenticado, em IPv4 e IPv6, para a sincronização do relógio com outros dispositivos de rede, garantindo a alta efetividade e segurança na troca de mensagens com os servidores de tempo; 31. Deve possuir interface USB para manipulação de arquivos com firmware ou configuração localmente; 32. Deve permitir configuração/administração remota através de SSH e SNMPv3; 33. Deve permitir a criação de três níveis de administração e configuração do switch. Permitir a autenticação de usuário de gerência em servidor RADIUS e TACACS+; 34. Deve implementar tecnologia para monitoramento de tráfego baseado em IPFIX, Netflow ou Netstream, garantindo alta visibilidade do tráfego de rede. Caso a análise seja feita por amostragem, deve ser suportada amostragem de 1 a cada 32 pacotes; 35. Deve permitir o envio de mensagens geradas pelo sistema em servidor externo (syslog), indicando a hora exata do acontecimento; 36. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática. Deve suportar fonte de alimentação redundante. Deve ser fornecido cabo de energia obedecendo o padrão NBR 14136; 37. Gabinete padrão para montagem em rack de 19", com altura máxima de 1U, incluindo todos os acessórios para o perfeito funcionamento; 38. O equipamento deve possuir garantia pelo período de 36 (trinta e seis) meses com envio de peças de reposição em até 3 dias úteis; - A garantia deve incluir o envio de equipamentos de reposição que deverão ser entregues nos locais especificados neste termo de referência. - Os serviços serão solicitados mediante a abertura de um chamado, via chamada telefônica 0800, e-mail, website ou chat da licitante vencedora, e, constatada a necessidade, a mesma deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante; - O atendimento aos chamados deve ser realizado em até um dia útil a partir da abertura do chamado. - A resolução do problema e/ou defeito registrado deverá ocorrer, no máximo, em 15 dias corridos a partir da abertura do chamado. - Caso seja necessário a substituição | | | | |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| | do equipamento, a mesma deverá ser realizada em até 30 dias corridos, a partir da constatação pela equipe técnica da licitante vencedora, dentro do prazo de 15 dias conforme descrito no item anterior; - A licitante vencedora deve indicar, na assinatura da Ata de Registro de Preços, os procedimentos para abertura de suporte técnico; - A licitante vencedora deve possuir, no momento da assinatura da Ata de Registro de Preços, pelo menos 1 (um) profissional com certificação técnica específica da tecnologia empregada (SWITCH) emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade; Comprovação através da apresentação da certificação. - A contratante poderá solicitar o escalonamento de incidentes ao fabricante do equipamento quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware; - A garantia iniciará sua contagem a partir da data de emissão da NF dos equipamentos, serviços ou licenças. - Prazo de entrega de produtos: no máximo 90 (noventa) dias corridos a partir da emissão de Autorização de Fornecimento pelo IFSC; - Os equipamentos devem possuir atualização de firmware pelo período de garantia sem custos adicionais, sob responsabilidade da empresa licitante vencedora; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas, não sendo aceitos equipamentos com caixas violadas. - Todos os equipamentos que necessitem de energia elétrica para seu funcionamento deverão vir acompanhados de cabos de alimentação conforme o padrão brasileiro – NBR 14136. - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. | | | | |
| 30 | SWITCH GERENCIÁVEL 8 PORTAS GIGABIT ETHERNET --> Switch Gerenciável 8 portas Gigabit Ethernet + 2 portas GBIC com as seguintes características: 8 portas Gigabit Ethernet 10/100/1000 Mbps + 2 portas Mini-GBIC; Porta Console; Gerenciável pela Web/SNMP; suporte a VLAN 802.1q e VLAN baseada em porta. Garantia: 12 meses. marca/modelo de referência: TP-LInk TL-SG3210 | UNIDADE | 69 | 707,96 | 48.849,24 |
| 31 | EQUIPAMENTO TIPO THIN CLIENT Processador: Intel Baytrail Quad Core 1.83ghz Ou Superior; Memória Ram: Ddr3 1333mhz De 2gb Ou Superior; Vídeo: 1x Saída Hdmi, Resolução Máxima 1920x1080x60hz – Fulhd Lan: 1x Ethernet Lan 10/100/1000mbps – Gigabits Wireless: 1x Wireless Lan Ieee 802.11b/G/N 300mbps Bluetooth: 1x Bluetooth 4.0 Audio: Realtek Alc887 – 7.1 High Definition 1x Line-On&Mic-In Usb: 4x Portas Usb 2.0 Armazenamento: Flash/Ssd – 32gb; Leitor De Cartão (MICROSD) Alimentação: Fonte De Alimentação Externa – Consumo 15w; Entrada 100~240v Automático / Saída 5v-3a; 1x Conector De Entrada De Alimentação (MINI Usb) Suporte Vesa: Plástico Suporte Vesa; Gabinete: Cor Preta & Prata Dimensão 17x100x85mm (AXLXP); Peso 0.180kg; Led's/Indicadores Led Ligado; Lan E Acionamento De Disco/ Indicadores De Todas As Portas Sistema Operacional: Linux (EMBARCADO) Clientes Vdi: Rdp Remote Fx; Citrix Hdx; Vmware Pcoip: Amazon Web Space; Go-Global: Navegador; Emulador Terminal; Vcn; Sw Gerenciamento; Acesso À Vdi: Userful Multiplataform-Multiseat Linux; Ltsp Certificados: Produto: Iec 60950; Iec 61000; Normativa Rohs; Anatel; Hcl; | UNIDADE | 160 | 1.140,67 | 182.507,20 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 32 | Videoconferência - Terminal de comunicação Tipo 01 Especificações Mínimas: 1. Terminal de comunicação IP composto por endpoint com capacidade de decoding/transcoding de áudio e vídeo, videocamera, microfone, controle remoto e acessórios para pleno funcionamento; 2. O conjunto deve ser nativo no protocolo IP. Não serão aceitos equipamentos que necessitem de adaptadores externos para o funcionamento; 3. O conjunto deve operar em ambientes de arquitetura de hardware dedicada para processamento de vídeo. Não serão aceitas soluções onde a base da arquitetura seja em formato de PC; 4. O conjunto deve permitir fixação em parede. Todos os acessórios devem ser incluídos; 5. A câmera deve apresentar as seguintes características técnicas: movimentação horizontal de, no mínimo, +25 a -25 graus; movimentação vertical de, no mínimo, +5 a – 20 graus; possuir zoom (óptico + digital) de pelo menos 4x; possuir foco automático; possuir controle de branco manual e automático; operar com resolução nativa mínima de 1080p30 (1920x1080 com 30 frames por segundo); 6. O equipamento deve implementar nativamente o protocolo SIP; 7. Deve suportar nativamente endereçamento nos protocolos IPv4 e IPv6; 8. Permitir velocidade de comunicação ponto-a-ponto de no mínimo 3Mbps de velocidade; 9. Transmissão de duas fontes independentes de vídeo, utilizando o padrão BFCP; 10. Deve guardar as informações de últimas chamadas realizadas, recebidas e perdidas. Deve possuir função de chamada em espera (Hold) e transferência de chamada para outro endpoint; 11. Deve acompanhar um microfone de mesa ou embutido no próprio equipamento. Deve permitir a instalação de um segundo microfone; 12. Deverá suportar os protocolos de áudio G.711, G.722, G.722.1 e G729; 13. Deverá suportar os protocolos de vídeo H.263 e H.264 e as resoluções 1080p com 30 frames por segundo e 720p com 30 frames por segundo; 14. Além da entrada de vídeo da câmera, deve possuir 1 (uma) entrada de vídeo exclusiva para conexão de dispositivos que possam compartilhar conteúdo na videoconferência. Esta entrada deve ser digital com conector HDMI e suportar resoluções HD 720p; 15. Deve possuir 1 (uma) saída para conexão do monitor principal, através de conexão digital (HDMI ou DVI), operando com resolução de 1080p60 (1920x1080 pixels); 16. Deve possuir 2 (duas) entradas de áudio, sendo 01 (uma) entrada através da própria interface HDMI e 01 (uma) entrada P2/mini-jack ou semelhante, para conexão de outros dispositivos. A entrada P2/mini-jack ou semelhante pode ser compartilhada com a entrada do microfone adicional; 17. Deve possuir 2 (duas) saídas de áudio, sendo 01 (uma) saída para o áudio principal no sistema digital HDMI (para conexão no sistema de tv/monitor) e 01 (uma) saída adicional P2/mini-jack ou semelhante para conexão em outros dispositivos como sistemas de som externos; 18. Deve implementar o protocolo IEEE 802.1Q; 19. Dever possuir uma interface ethernet com velocidade 100 Mbps e conector RJ-45 diretamente no equipamento; 20. Deve permitir ser gerenciado por um controlador de chamadas; 21. Deve permitir a atualização de firmware através do próprio controlador de chamadas; 22. Suporte a QoS conforme o padrão IEEE 802.1p com DiffServ; 23. Possuir gerenciamento remoto via HTTPS e SSH; 24. Deve implementar 802.1x com pelo menos EAP-TLS; 25. Serviço de segurança através de criptografia, baseado nos modelos AES com criação automática de chaves de autenticação; 26. Deve possuir cliente DHCP, permitindo configuração automática de endereçamento IP. Deve suportar também a configuração manual de endereçamento IP; 27. Permitir o uso de papel de parede customizado, de forma a padronizar todos os terminais que forem adquiridos; 28. Deve suportar alimentação através de PoE. Caso o equipamento não opere com alimentação PoE, deve ser fornecida fonte de alimentação (interna ou externa, com capacidade de operação 100-240VAC); 29. Deve ser homologado pela ANATEL; 30. Deve ser garantida atualização de software/firmware do equipamento pelo período de garantia sem custos para este órgão; 31. Garantia de 36 (trinta e seis) meses com primeiro atendimento em até 1 dia útil e envio de peças defeituosas e/ou equipamento em até 3 dias úteis. - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. Modelo de referência: Cisco SX10 | EQUIPAMENTO | 3 | 21.641,85 | 64.925,55 |

| Item | Descrição | Unidade | Quant. | Preço Unit. (R$) | Valor Total (R$) |
|---|---|---|---|---|---|
| 33 | Videoconferência - Terminal de comunicação Tipo 02 Especificações Mínimas: 1. Terminal de comunicação IP composto por endpoint com capacidade de decoding/transcoding de áudio e vídeo, videocamera, microfone de mesa, controle remoto e acessórios para pleno funcionamento; 2. O conjunto deve ser nativo no protocolo IP. Não serão aceitos equipamentos híbridos com telefonia analógica ou que necessitem de adaptadores externos para o funcionamento; 3. O conjunto deve operar em ambientes de arquitetura de hardware dedicada para processamento de áudio e vídeo. Não serão aceitas soluções onde a base da arquitetura seja em formato de PC; 4. O equipamento deve implementar nativamente o protocolo SIP e H.323, estando licenciado para operação com os dois protocolos; 5. Deve suportar nativamente os protocolos IPv4 e IPv6; 6. Deve conectar-se à rede através de uma entrada Ethernet 802.3, conector padrão RJ-45 e velocidade de 100/1000 Base-T; 7. Deve implementar o protocolo IEEE 802.1Q; 8. Permitir velocidade de comunicação ponto-a-ponto a 6Mbps de velocidade ou superiores; 9. A câmera deve ser totalmente separada do codec e apresentar as seguintes características técnicas: movimentação horizontal de +85 a -85 graus; movimentação vertical de +9 a – 25 graus; possuir zoom óptico de pelo menos 12x; possuir foco automático; possuir controle de branco manual e automático; operar com resolução nativa mínima de 1080p60 (1920x1080 com 60 frames por segundo); deve ser totalmente compatível com o codec de videoconferência proposto e do mesmo fabricante; 10. O codec deve apresentar as seguintes características técnicas: 11. Transmissão de duas fontes independentes de vídeo, utilizando os padrões H.239 e BFCP; 12. No caso de transmissão de duas fontes de vídeo (utilizando o protocolo H.239 ou BFCP) e caso esteja sendo utilizado dois monitores, possibilitar a configuração de layout da tela para que em um dos monitores apareça o vídeo do participante remoto e no outro monitor apareça o compartilhamento que esteja sendo realizado; 13. Deverá implementar os protocolos de vídeo H.263 e H.264; 14. Deve implementar resoluções 1080p com 60 frames por segundo e 720p com 60 frames por segundo; 15. Deve possuir duas interfaces digitais para entrada de vídeo, podendo ser DVI ou HDMI e que permita a sua utilização em resolução 1080p (1920x1080 pixels); 16. Deve permitir a utilização de dois monitores simultaneamente, devendo para isso possuir no mínimo 02 (duas) saídas de vídeo, sendo 1 (uma) saída para monitor principal, através de conexão digital HDMI ou equivalente, operando com resolução de 1080p (1920x1080 pixels); e 1 (uma) saída para monitor secundário, através de conexão digital HDMI ou equivalente, com resolução de 1080p (1920x1080 pixels); 17. Deverá suportar os protocolos de áudio G.711, G.722, G.722.1; 18. Deve possuir 03 (três) entradas de áudio, sendo 02 (duas) entradas independentes para microfone de mesa e 01 (uma) entrada auxiliar analógica mono ou estéreo, para conexão de outros dispositivos; 19. Deve possuir 02 (duas) saídas de áudio, sendo 01 (uma) saída para o áudio principal no sistema digital HDMI e 01 (uma) saída estéreo, para conexão a outros dispositivos ou sistema de som; 20. Permitir registro e autenticação em gatekeepers e SIP proxies/registrars simultaneamente; 21. Deve possuir hardware preparado para MCU interna permitindo a realização de uma chamada com no mínimo mais 3 terminais de vídeo. Esta funcionalidade deve implementar transcodificação individual, permitindo a participação de terminais com codificações diferentes. Caso seja licenciável, tal licença não precisa ser fornecida neste processo; 22. Deve guardar as informações de últimas chamadas realizadas, recebidas e perdidas. Deve possuir função de chamada em espera (Hold) e transferência de chamada para outro endpoint; 23. Deve suportar H.245 para envio de tons DTMF em H.323; 24. Suporte a QoS conforme o padrão IEEE 802.1p com DiffServ; 25. Suporte aos protocolos H.460.18 e H.460.19 (travessia transparente de Firewalls); 26. Possuir gerenciamento remoto pelo menos via web browser e SSH; 27. Serviço de segurança através de criptografia, baseado nos modelos AES, com criação automática de chaves de autenticação; 28. Deve implementar 802.1x com pelo menos EAP-TLS; 29. Permitir o uso de papel de parede customizado, de forma a padronizar todos os terminais que forem adquiridos; 30. O codec deverá possuir fonte de alimentação operando automaticamente em 100 a 240V, 50 e 60Hz; 31. Equipamento deve possuir interface do usuário em português brasileiro; 32. Deve ser homologado pela ANATEL; 33. Deve ser garantida atualização de software/firmware do equipamento pelo período de garantia sem custos para este órgão; 34. Garantia de 36 (trinta e seis) meses com primeiro atendimento em até 1 dia útil e envio de peças defeituosas e/ou equipamento em até 3 dias úteis. - PROPOSTA - Apresentar catálogo técnico oficial do produto, do Fabricante, que apresente as características técnicas em conformidade com as descritas no Projeto Básico e seus Anexos em todos os seus itens, sem exceção, sendo que cada item exigido deverá estar grifado em destaque neste catálogo, a fim de facilitar a identificação; - Apresentar a "repetição" deste conjunto de especificações na proposta técnica não garante o seu atendimento integral. Não serão consideradas afirmações sem a devida comprovação; - Deverá informar site onde se encontra o catálogo para confirmação das características do equipamento. Modelo de referência: Cisco SX20 | EQUIPAMENTO | 6 | 55.623,82 | 333.742,92 |

**Valor Total do Processo: R$ 8.338.142,84**