INSTITUTO FEDERAL Santa Catarina
Compras

INSTITUTO FEDERAL DE SANTA CATARINA
SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS
PRÓ-REITORIA DE DESENVOLVIMENTO INSTITUCIONAL
DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO
EMITIDO EM 08/09/2021 08:31

RELATÓRIO DOS ITENS COM AS REQUISIÇÕES

Licitação: 23292.010214/2021-24 - PE 32/2021 - REI
Gestora: 1100 - REI
Assunto: AQUISIÇÃO DE SOLUÇÃO UNIFICADA DE SEGURANÇA E CONECTIVIDADE SEM FIO
Tipo: MATERIAIS
Status: SETOR DE COMPRAS - EM ANALISE - SETOR COMPRAS

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
1	**44905237001000060 - CATMAT: 0**	**UNIDADE**	--	--	--	15	0	15	--	--
	SWITCH TIPO 2 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA SWITCH TIPO 2 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA ---> Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo); 6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 7. Deve possuir tabela MAC com suporte a 8.000 endereços; 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 10. Deve suportar a comutação de Jumbo Frames; 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 10.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 14. Deve implementar serviço de DHCP Relay; 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela; 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 19. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 27. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 31. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 34. Deve suportar MAC Authentication Bypass (MAB); 35. Deve implementar RADIUS CoA (Change of Authorization); 36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 37. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 39. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 42. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 43. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 44. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 46. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 51. Deve permitir ser gerenciado através de IPv6; 52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 54. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 58. Deverá suportar ser configurado e monitorado através de REST API; 59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 60. Deve suportar temperatura de operação de até 45º Celsius; 61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 62. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 64. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).								
	1275/2021 / 111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO				15			
2	**44905237001000061 - CATMAT: 0**	**UNIDADE**	--	--	--	15	0	15	--	--

TOTAL LICITADO: **R$ 0,00**

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
3	**SWITCH TIPO 3 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA** SWITCH TIPO 3 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 180W; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 8.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 28. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 1275/2021 / 111702 / DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	**449052370010000620 - CATMAT: 0**	**UNIDADE**	--	--	--	**15**	**0**	**15**	--	--

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
4	**44905237001000063 - CATMAT: 0** **SWITCH TIPO 4 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA** Switch Tipo 4 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W a serem alocados em qualquer uma das portas 1000Base-T; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 8.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 28. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 1275/2021 / 111702 / DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	**UNIDADE**	--	--	--	**15**	**0**	**15**	--	--

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
5	**SWITCH TIPO 5 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA** SWITCH TIPO 5 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir capacidade de comutação de pelo menos 104 Gbps e ser capaz de encaminhar até 150 Mpps (milhões de pacotes por segundo); 6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 7. Deve possuir tabela MAC com suporte a 16.000 endereços; 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 10. Deve suportar a comutação de Jumbo Frames; 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 14. Deve implementar serviço de DHCP Relay; 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 19. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 27. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 31. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 34. Deve suportar MAC Authentication Bypass (MAB); 35. Deve implementar RADIUS CoA (Change of Authorization); 36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 37. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 39. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 42. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 43. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 44. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 46. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 51. Deve permitir ser gerenciado através de IPv6; 52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 54. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 58. Deverá suportar ser configurado e monitorado através de REST API; 59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 60. Deve suportar temperatura de operação de até 45º Celsius; 61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 62. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 64. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 1275/2021 / 111702	**44905237001000064 - CATMAT: 0**	**UNIDADE**	--	--	--	**15**	**0**	**15**	--	--
			DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			15				

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

SWITCH TIPO 6 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA
SWITCH TIPO 6 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 104 Gbps e ser capaz de encaminhar até 150 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 16.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 28. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		15				

6	5235003000921 - CATMAT: 0	UNIDADE	--	--	--	20	0	20	--	--

TRANSCEIVER 1000BASE-SX
TRANSCEIVER 1000BASE-SX 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 1000BASE-SX para fibras ópticas de até 400 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		20				

7	5235003000922 - CATMAT: 0	UNIDADE	--	--	--	20	0	20	--	--

TRANSCEIVER 1000BASE-LX
TRANSCEIVER 1000BASE-LX 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 1000BASE-X para fibras ópticas de até 10 kilometros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		20				

8	5235003000923 - CATMAT: 0	UNIDADE	--	--	--	20	0	20	--	--

TRANSCEIVER 10GBASE-SR
TRANSCEIVER 10GBASE-SR 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de até 300 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		20				

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
9	**5235003000924 - CATMAT: 0** **TRANSCEIVER 10GBASE-LR** TRANSCEIVER 10GBASE-LR 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas de até 10 kilometros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 1275/2021 / 111702 / DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	**UNIDADE**	--	--	20	0	20	--	--
10	**44904005001000087 - CATMAT: 0** **FERRAMENTA DE GERENCIAMENTO CENTRALIZADO – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA** FERRAMENTA DE GERENCIAMENTO CENTRALIZADO – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede dos campus e que garanta suporte a processos relativos à LGPD; 2. Deverá ser totalmente compatível com a solução proposta para gerenciamento da segurança e infraestrutura de rede dos campus; 3. A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato; 4. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 5. A solução deverá ser composta por elemento ou elementos fornecido(s) na forma de appliance virtual (máquina virtual) compatível com Vmware ESXi, Microsoft Hyper-V ou Linux KVM; 6. A solução deverá garantir a integridade da configuração de um determinado item através de bloqueio de alterações quando ocorrer acesso simultâneo de dois ou mais administradores no mesmo ativo; 7. A solução deverá possibilitar a criação e administração de políticas de firewall, controle de aplicação e filtro de URL; 8. A solução deverá permitir criar, de forma centralizada, novos objetos que poderão ser utilizados nas políticas; 9. A solução deverá permitir que o administrador localize em quais regras um determinado objeto (ex: computador, serviço, etc.) está sendo utilizado; 10. A solução deverá atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS; 11. A solução deverá permitir a criação de regras de filtragem de tráfego que fiquem ativas apenas em horários pré-definidos; 12. A solução deverá permitir a criação de regras de filtragem de tráfego com data de expiração; 13. A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso; 14. A solução deve permitir a criação de templates de configuração de túneis VPN IPSec a serem aplicados de maneira centralizada e padronizada em elementos concentradores VPN; 15. A solução deve permitir agendamento para a execução de configurações nos elementos administrados; 16. A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada; 17. A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches; 18. As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID; 19. As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso; 20. As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de wIDS ou wIPS; 21. As seguintes características de Bluetooth Low Energy (BLE) devem ser configuradas nos pontos de acesso através dos templates: configuração do UUID, Major ID, Minor ID, Beacon Interval e potência; 22. As seguintes características de VLAN devem ser configuradas nos switches através dos templates: VLAN, VLAN ID e endereçamento IP; 23. As seguintes características de segurança devem ser configuradas nos switches através dos templates: Autenticação 802.1X, Autenticação MAB e Guest VLAN; 24. As seguintes características de rede devem ser configuradas nos switches através dos templates: configuração das portas com respectivas VLANs tagged e untagged, configuração do protocolo LLDP e configurações de QoS; 25. A solução deve permitir que o administrador selecione em quais elementos os templates de configuração deverão ser aplicados; 26. A solução deve listar os elementos adminstrados e seu status de operação; 27. A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID; 28. A solução deve listar todos os Rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP; 29. A solução deve incorporar mapa mundi para visão unificada do status de operação dos elementos. Deve ainda permitir a adição de planta baixa de múltiplas localidades; 30. A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches; 31. A solução deve apresentar a topologia da rede com status dos elementos e informações sobre a atuação do protocolo Spanning-Tree em interfaces; 32. A solução deve permitir a execução de testes remotos para identificação de problemas em cabos de rede conectados aos switches; 33. A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração; 34. A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente; 35. A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas; 36. A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada; 37. A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada; 38. A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados. Deve permitir ainda que o administrador da rede agende a atualização da versão de firmware de maneira automática nos elementos administrados; 39. A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio; 40. A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos; 41. A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos; 42. A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados; 43. A solução deve garantir visão centralizada das estatísticas de uso dos túneis VPN, com informações sobre volume de dados trafegados, horário da conexão e identificação do usuário que conectou na VPN; 44. A solução deverá ser capaz de receber os logs dos elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede das unidades e apresenta-los de forma centralizada; 45. A solução deverá ser capaz de receber, no mínimo, 5GB de logs diários; 46. A solução deverá ser capaz de armazenar, no mínimo, 3TB de informação; 47. A solução deverá ser capaz de armazenar os logs por 12 meses; 48. A solução deverá possuir mecanismo para que logs antigos sejam removidos automaticamente; 49. A solução deverá permitir a exportação dos logs; 50. A solução deverá permitir que o administrador realize download de um determinado conjunto de logs em formato texto ou CSV; 51. A solução deverá garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego; 52. A solução deverá permitir a extração de relatórios; 53. A solução deverá possuir relatórios pré-definidos; 54. A solução deverá possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida; 55. A solução deverá permitir a personalização de capas para os relatóri 56. A solução deverá permitir a geração de relatórios de logs de tráfego de dados; 57. A solução deverá permitir a personalização dos relatórios para inserção de gráficos dos tipos barra, linha, tabela e pizza; 58. A solução deverá possibilitar o envio de relatórios por e-mail de maneira automática; 59. A solução deverá permitir a customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da contratante, adaptando-o às suas necessidades; 60. A solução deverá permitir a definição de filtros nos relatórios; 61. A solução deverá ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros; 62. A solução deverá garantir a capacidade de criar consultas avançadas em sua base de dados que para as informações sejam utilizadas em gráficos e tabelas dentro dos relatórios; 63. A solução deverá implementar autenticação administrativa através do protocolos RADIUS ou TACACS; 64. A solução deverá permitir a criação de múltiplos perfis de usuários administradores com permissões granulares para limitar o acesso a determinadas funções e garantir privilégios de somente leitura e/ou leitura-escrita a outras; 65. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7. Durante o período de garantia deve ser possível a atualização do software para novas versões. 1276/2021 / 111702 / DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	**LICENÇA**	--	--	2	0	2	--	--
11	**33904021012000151 - CATMAT: 0**	**SERVIÇO**	--	--	10	0	10	--	--

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

UNIDADE DE SERVIÇO TÉCNICO PARA SITE SURVEY
UNIDADE DE SERVIÇO TÉCNICO PARA SITE SURVEY 1. O serviço de Site Survey será utilizado para análise técnica do ambiente real dos campus do IFSC em todas as localidades do estado de Santa Catarina de forma presencial nos respectivos endereços, apoiada por ferramentas e softwares adequados, que indiquem: 1.1. O melhor posicionamento dos dispositivos pontos de acesso de rede sem fio para a maximização da cobertura do sinal de RF; 1.2. A quantidade exata de pontos de acesso a serem instalados por prédio; 1.3. Fontes e zonas de interferência; 1.4. O canal de frequência a ser utilizado por cada ponto de acesso; 1.5. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF em desenho colorido; 2. A unidade de serviço deve contemplar um campus independente da sua localidade; 3. Será de responsabilidade da CONTRATANTE a disponibilização de planta arquitetônica em CAD (*.dwg) para realização de predição teórica e confecção de as-built; 4. Será de responsabilidade da CONTRATADA os seguintes serviços abaixo: 4.1. A disponibilização de um ou mais técnicos para realização de testes em campos para determinar a melhor disposição dos pontos de acesso de rede sem fio; 4.2. Relatório técnico de vistoria resultante da predição teórica das plantas fornecidas pela CONTRATANTE com as seguintes informações: 4.2.1. As possíveis limitações físicas ou dificuldades de implementação detectados nos locais – restrições da construção, obstáculos, etc.; 4.2.2. Melhor posicionamento dos dispositivos em cada andar das localidades visando a maximização da cobertura do sinal de RF; 4.2.3. A quantidade exata de pontos de acesso a ser instalados em cada andar e locais previstos no projeto; 4.2.4. As zonas e faixas de interferência detectadas durante o mapeamento de rádio frequência; 4.2.5. As faixas de frequência a serem utilizadas para cada ponto de acesso; 4.2.6. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF avaliados durante o mapeamento; 5. O relatório técnico deverá ser emitido com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 6. Todos os instrumentos/equipamentos e softwares necessários para a execução do serviço serão fornecidos pela CONTRATADA; 7. O relatório técnico de vistoria com o resultado do estudo de site survey deverá ser entregue ao analista ou técnico de TI lotados no câmpus em avaliação, em via impressa ou em meio digital em até 30 (trinta) dias úteis após assinatura do contrato para os itens acima citados.

1277/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	10

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
12	339040210060000152 - CATMAT: 0	SERVIÇO	--	--	--	10	0	10	--	--

SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPOS 1, 2, 3 E 4
SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPOS 1, 2, 3 E 4 --> Características Mínimas: 1. Entende-se por configuração da solução a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CONTRATANTE; 2. O serviço deverá contemplar a configuração de uma unidade da Solução de gerenciamento de redes e segurança para campus tipos 1, 2, 3 ou 4 especificados nesse processo; 3. Deverá contemplar também a adição do(s) dispositivo(s) da solução na ferramenta de gerenciamento centralizado; 4. O serviço de configuração poderá ser realizado de maneira 100% remota, desde que devidamente acordado e documentado entre a CONTRATANTE e a CONTRATADA; 5. São de responsabilidade da CONTRATADA, entre outras atividades: 5.1. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos firewalls em produção no ambiente atual para a nova solução; 5.2. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões; 5.3. Configurar as funcionalidades relevantes a implementação da solução como: Endereçamento, VLANs, LACP, DHCP e tipos NAT; 5.4. Configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF; 5.5. Realizar a configuração das políticas de firewall analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários e grupos de usuários; 5.6. Implementar políticas de bloqueios de arquivos; 5.7. Configurar limitações de banda com base no IP de origem, usuários e grupos; 5.8. Configurar regras de IPS, Anti-Malware e Filtro URL; 5.9. Configuração da ferramenta de gerenciamento centralizado; 5.10. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório da CONTRATANTE, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação; 5.11. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado; 5.12. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser; 5.13. Configuração das assinaturas de wIDS/Wips; 5.14. Configuração de políticas de bloqueio de rogue APs; 5.15. Configuração para classificação/detecção de interferências WiFi e não-WiFi; 5.16. Configuração dos pontos de acesso sem fio; 5.17. Configuração de SSIDs; 5.18. Configuração do controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança; 5.19. Configuração de um portal de autenticação web para os usuários visitantes, com as seguintes funcionalidades: 5.19.1. Funcionar de forma criptografada com o uso de certificados (SSL); 5.19.2. Customizar com logotipo e políticas de acesso; 5.19.3. Check-box para aceite com as políticas de acesso da rede; 6. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 7. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 8. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 9. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 10. A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE; 11. Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI; 12. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 13. O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia; 14. A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta; 15. Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a “DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO” contendo todas as informações da implantação: 15.1. Aspecto da arquitetura implantada; 15.2. Configuração; 15.3. Descrição das características e recursos utilizados; 15.4. Testes e integração dos ambientes de redes locais da instalação; 16. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 17. A documentação poderá ser entregue em via impressa ou meio digital; 18. A documentação deverá validada pela equipe técnica da CONTRATANTE; 19. Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRADADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE; 20. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formado de repasse de conhecimentos com carga horaria mínima de 8 horas;

1277/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	10

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
13	339040210060000153 - CATMAT: 0	SERVIÇO	--	--	--	1	0	1	--	--

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
	SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5 SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5 1. Entende-se por configuração da solução a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CONTRATANTE; 2. O serviço deverá contemplar a configuração de uma unidade da Solução de gerenciamento de redes e segurança para campus tipo 5 e a instalação e configuração da ferramenta de gerenciamento centralizado especificado nesse processo; 3. O serviço de configuração poderá ser realizado de maneira 100% remota, desde que devidamente acordado e documentado entre a CONTRATANTE e a CONTRATADA; 4. São de responsabilidade da CONTRATADA, entre outras atividades: 4.1. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos firewalls em produção no ambiente atual para a nova solução; 4.2. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões; .4.3. Configurar as funcionalidades relevantes a implementação da solução como: Endereçamento, VLANs, LACP, DHCP e tipos NAT; 4.4. Configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF; 4.5. Realizar a configuração das políticas de firewall analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários e grupos de usuários; 4.6. Implementar políticas de bloqueios de arquivos; 4.7. Configurar limitações de banda com base no IP de origem, usuários e grupos; 4.8. Configurar regras de IPS, Anti-Malware e Filtro URL; 4.9. Configuração da ferramenta de gerenciamento centralizado; 4.10. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório da CONTRATANTE, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação; 4.11. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado; 4.12. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser; 4.13. Configuração das assinaturas de wIDS/Wips; 4.14. Configuração de políticas de bloqueio de rogue APs; 4.15. Configuração para classificação/detecção de interferências WiFi e não-WiFi; 4.16. Configuração dos pontos de acesso sem fio; 4.17. Configuração de SSIDs; 4.18. Configuração do controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança; 4.19. Configuração de um portal de autenticação web para os usuários visitantes, com as seguintes funcionalidades: 4.19.1. Funcionar de forma criptografada com o uso de certificados (SSL); 4.19.2. Customizar com logotipo e políticas de acesso; 4.19.3. Check-box para aceite com as políticas de acesso da rede; 5. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 6. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 7. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 8. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 9. A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE; 10. Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia; 13. A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta; 14. Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a “DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO” contendo todas as informações da implantação: 14.1. Aspecto da arquitetura implantada; 14.2. Configuração; 14.3. Descrição das características e recursos utilizados; 14.4. Testes e integração dos ambientes de redes locais da instalação; 15. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 16. A documentação poderá ser entregue em via impressa ou meio digital; 17. A documentação deverá validada pela equipe técnica da CONTRATANTE; 18. Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRADADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE; 19. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formado de repasse de conhecimentos com carga horaria mínima de 8 horas;								
	1277/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		1				
14	**5230005000239 - CATMAT: 0**	**UNIDADE**	**--**	**--**	**270**	**0**	**270**	**--**	**--**
	INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 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 os pontos de acesso deste processo 3. Deve fornecer no mínimo 30 Watts para alimentação do dispositivo com suporte PoE atendendo ao padrão IEEE 802.3at; 4. Deve acompanhar cabos de energia e acessórios para o seu perfeito funcionamento; 5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática. Deve acompanhar o cabo de alimentação; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).******** Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012.								
	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		270				
15	**44905237001000059 - CATMAT: 0**	**UNIDADE**	**--**	**--**	**6**	**0**	**6**	**--**	**--**

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
160	**SWITCH TIPO 1 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA** SWITCH TIPO 1 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir 1 (uma) interface USB; 6. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 260 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 32.000 endereços; 9. Deve operar com latência igual ou inferior à 1us (microsegundo); 10. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 11. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente; 12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 13. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos os switches como uma única interface lógica; 14. Deve suportar a comutação de Jumbo Frames; 15. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 16. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 17. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 18. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos; 19. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 20. Deverá suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 21. Deve implementar serviço de DHCP Server e DHCP Relay; 22. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 23. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN); 24. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN; 25. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 26. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 27. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 28. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 29. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 30. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 31. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 32. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 33. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 34. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 35. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 36. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ); 37. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 38. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados; 39. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement; 40. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 41. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 42. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 43. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 44. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 45. Deve suportar MAC Authentication Bypass (MAB); 46. Deve implementar RADIUS CoA (Change of Authorization); 47. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 48. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 49. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 50. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 51. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 52. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 53. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 54. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 55. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 56. Deve ser capaz de autorizar a transmissão de pacotes nas interfaces somente para aqueles endereços IP que foram aprendidos dinamicamente através de DHCP Snooping. Os pacotes originados por endereços IP desconhecidos deverão ser descartados; 57. Deve suportar o protocolo PTP (Precision Time Protocol); 58. Deve implementar Netflow, sFlow ou similar; 59. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 60. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 61. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 62. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 63. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 64. Deve permitir ser gerenciado através de IPv6; 65. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 66. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 67. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 68. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 69. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo; 70. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 71. Deverá suportar ser configurado e monitorado através de REST API; 72. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark; 73. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash; 74. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE); 75. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 76. Deve suportar temperatura de operação de até 45º Celsius; 77. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 78. Deve ser fornecido com fontes de alimentação redundantes e internas ao equipamento, com capacidade para operar em tensões de 110V e 220V; 79. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 80. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 81. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 82. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 83. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 1275/2021 / 111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			6				
160	**449052370010000580 - CATMAT:**	**UNIDADE**	--	--	--	**250**	**0**	**250**	--	--

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								
17	**44905237001000057 - CATMAT: 0** **PONTO DE ACESSO INDOOR – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA** PONTO DE ACESSO INDOOR – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio; 21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA; 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 31. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea; 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; 39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 42. Deve implementar o padrão IEEE 802.11e; 43. Deve implementar o padrão IEEE 802.11h; 44. Deve implementar o padrão IEEE 802.3az; 45. Deve suportar ser gerenciado via SNMP; 46. Deve suportar consultas via REST API; 47. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação; 48. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C; 49. Deve suportar sistema antifurto do tipo Kensington Security Lock ou similar; 50. Deve possuir indicadores luminosos (LED) para indicação de status; 51. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 52. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 53. Deve possuir certificado emitido pela Wi-Fi Alliance; 54. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 55. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 1275/2021 / 111702	**UNIDADE** DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	--	--	--	**20** 250	**0**	**20**	--	--

TOTAL LICITADO: **R$ 0,00**

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

PONTO DE ACESSO OUTDOOR - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA
PONTO DE ACESSO OUTDOOR - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio; 21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL); 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve implementar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 31. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 32. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea; 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X; 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 39. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 40. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 41. Deve implementar o padrão IEEE 802.11e; 42. Deve implementar o padrão IEEE 802.11h; 43. Deve implementar o padrão IEEE 802.3az; 44. Deve suportar consultas SNMP diretamente no ponto de acesso; 45. Deve suportar consultas REST API diretamente no ponto de acesso; 46. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes; 47. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60º C; 48. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção; 49. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios Wi-Fi; 50. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 51. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 52. Deve possuir certificado emitido pela Wi-Fi Alliance; 53. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 54. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		20				

18	**449052370010000052 - CATMAT: 0**	**UNIDADE**	**--**	**--**	**--**	**2**	**0**	**2**	**--**	**--**

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 1
SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 1---> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 5 (cinco) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 288 (duzentos e oitenta e oito) portas de switch ou um total de 6 (seis) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 8 (oito) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 1.6 Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 300 (trezentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 800 (oitocentos) Mbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 4.2 Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 400.000 (quatrocentas mil) de sessões simultâneas/concorrentes e 28.000 (vinte e oito mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021 / 111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			2				

19	**449052370010000053 - CATMAT: 0**	**UNIDADE**	**--**	**--**	**--**	**12**	**0**	**12**	**--**	**--**

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 2

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 2 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 8 (oito) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX;; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 672 (seiscentos e setenta e duas) portas de switch ou um total de 14 (quatorze) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 30 (trinta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 1.6 Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 600 (seiscentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 1.5 Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução dev erá ser capaz de tratar 6.2 Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 600.000 (seiscentas mil) de sessões simultâneas/concorrentes e 30.000 (trinta mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		12				

20	**44905237001000054 - CATMAT: 0**	**UNIDADE**	**--**	**--**	**--**	**6**	**0**	**6**	**--**	**--**

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 3

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 3 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 10 (dez) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 672 (seiscentos e setenta e duas) portas de switch ou um total de 14 (quatorze) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 40 (quarenta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 3.2 Gbps de tráfego encapsulado via VPN; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 3.74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 700 (setecentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 1.5 Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 9 (nove) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 1.400.000 (um milhão e quatrocentas mil) de sessões simultâneas/concorrentes e 40.000 (quarenta mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição **Unidade** **Unidade Gestora**								

servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		6				
21	**449052370010000550 - CATMAT: UNIDADE**		--	--	--	**6**	**0**	**6**	--	--

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 4

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 4 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 2 (duas) interfaces 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede; 4. Cada appliance físico deve possuir fontes de alimentações redundantes com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar os cabos de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 1440 (um mil, quatrocentas e quarenta) portas de switch ou um total de 30 (trinta) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 60 (sessenta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 3.2 Gbps de tráfego encapsulado via VPN; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 900 (novecentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 2 (dois) Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 16 (dezesseis) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 1.400.000 (um milhão e quatrocentas mil) de sessões simultâneas/concorrentes e 50.000 (cinquenta mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		6				
22	**449052370010000560 - CATMAT: 0**	**UNIDADE**	--	--	--	**1**	**0**	**1**	--	--

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5

SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 4 (quatro) interfaces 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X ou superior para permitir a conexão com a rede; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 3360 (três mil, trezentos e sessenta) portas de switch ou um total de 70 (setenta) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 500 (quinhentos) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A A solução deverá ser capaz de encaminhar 9 (nove) Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição / Unidade / Unidade Gestora								

VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 4.5 Gbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 14 (quatorze) Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 35 (trinta e cinco) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 7.000.000 (sete milhões) de sessões simultâneas/concorrentes e 400.000 (quatrocentas mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).

	1275/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		1				

23	**5230004000241 - CATMAT: 454271**	**UNIDADE**	--	--	--	**10**	**0**	**10**	--	--

NOBREAK 10 KVA - TORRE

NOBREAK 10 KVA - TORRE Características mínimas: Potência →10 kVA /10 kW; Tensão entrada → 115/220V~ (Bivolt); Tensão saída → 110/220V (De acordo com a solicitação de cada Câmpus indicada em AF); Fator de potência de saída →1; Conexão de entrada → bornes; Conexão de saída → Bornes + 8 tomadas NBR 14136 (20A); Formato → Torre; Transformador → Isolador; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Tempo de autonomia → 20 minutos no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008.

	1279/2021	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO		10				

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item / Requisição / Unidade / Unidade Gestora	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
24	**5230004000243 - CATMAT: 296659** **NOBREAK 3KVA - RACK** NOBREAK 3KVA - RACK Características mínimas: Potência →3 kVA / 2,7 kW; Tensão entrada → 220V; Tensão saída → 220V; Fator de potência de saída → 0,9 ou superior; Conexão de entrada → Plugue NBR 14136 (20A); Conexão de saída → 6 tomadas NBR 14136 (20A); Formato → Rack (2U); Fusível →Rearmável; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Tempo de autonomia → 20 min, no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008. 1279/2021 111702 DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	**UNIDADE**	--	--	--	**10**	**0**	**10**	--	--
25	**5230004000245 - CATMAT: 410388** **NOBREAK 3KVA - TORRE** NOBREAK 3KVA - TORRE Características mínimas: Potência →3 kVA / 2,7 kW; Tensão entrada → 115/220V~ (Bivolt); Tensão saída → 110/220V (De acordo com a solicitação de cada Câmpus indicada em AF); Fator de potência de saída → 0,9 ou superior; Conexão de entrada → Plugue NBR 14136 (20A) + bornes; Conexão de saída → Bornes + 8 tomadas NBR 14136 (20A); Formato → Torre; Transformador → Isolador; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Fusível →Rearmável; Tempo de autonomia → 20 min, no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008. 1279/2021 111702 DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	**UNIDADE**	--	--	--	**10**	**0**	**10**	--	--
26	**5230004000247 - CATMAT: 386679** **NOBREAK 6KVA - TORRE** NOBREAK 6KVA - TORRE Características mínimas: Potência →6 kVA /6 kW; Tensão entrada → 115/220V~ (Bivolt); Tensão saída → 110/220V (De acordo com a solicitação de cada Câmpus indicada em AF); Fator de potência de saída →1; Conexão de entrada → bornes; Conexão de saída → Bornes + 8 tomadas NBR 14136 (20A); Formato → Torre; Transformador → Isolador; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Tempo de autonomia → 20 min, no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008. 1279/2021 111702 DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	**UNIDADE**	--	--	--	**10**	**0**	**10**	--	--

TOTAL LICITADO: **R$ 0,00**

SIPAC | DTIC - Diretoria de Tecnologia da Informação e Comunicação - (48) 3877-9000 | Copyright © 2005-2021 - UFRN - appdocker1-srv1.appdocker1-inst1

PREGÃO ELETRÔNICO

Nº 32/2021

OBJETO: AQUISIÇÃO DE SOLUÇÃO SOLUÇÃO UNIFICADA DE SEGURANÇA E CONECTIVIDADE SEM FIO PARA O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, IFSC.

DATA DA ABERTURA: XX/XX/20XX às XXh

LOCAL: www.comprasnet.gov.br

FONE: (XX) XXXX-XXXX – FAX (XX) XXXX-XXXX

PREGÃO ELETRÔNICO
INSTITUTO FEDERAL DE SANTA CATARINA

PREGÃO ELETRÔNICO Nº 32/2021
(Processo Administrativo n° 23292.010214/2021-24)

Torna-se público, para conhecimento dos interessados, que o INSTITUTO FEDERAL DE SANTA CATARINA – IFSC, por meio do Departamento de Compras, sediado na Rua 14 de Julho, n. 150, CEP 88075-010, Coqueiros, Florianópolis, SC, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, com critério de julgamento ***menor preço por grupo***, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº **10.024, de 20 de setembro de 2019,** do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7892, de 23 de janeiro e 2013, da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, da Instrução Normativa SEGES/MP nº 03, de 26 de abril, de 2018, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, e as exigências estabelecidas neste Edital.

Data da sessão: XX/XX/20XX
Horário: XX:XXh
Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br

1 DO OBJETO

1.1 O objeto da presente licitação é a escolha da proposta mais vantajosa para a **AQUISIÇÃO DE SOLUÇÃO UNIFICADA DE SEGURANÇA E CONECTIVIDADE SEM FIO,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2 A licitação será dividida em grupos, formados por um ou mais itens**,** conforme tabela constante no Termo de Referência, facultando-se ao licitante a participação em quantos grupos forem de seu interesse, devendo oferecer proposta para todos os itens que o compõem.

1.3 O critério de julgamento adotado será o menor preço GLOBAL do grupo, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2 DO REGISTRO DE PREÇOS

2.1 As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços

3 DO CREDENCIAMENTO

3.1 O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2 O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

3.3 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.5 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

4 DA PARTICIPAÇÃO NO PREGÃO

4.1 Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018 com o seguinte nível de cadastramento:

I. Credenciamento;
II. Habilitação Jurídica;
III. Regularidade fiscal federal;
IV. Regularidade fiscal estadual/municipal;
V. Qualificação Técnica
VI. Qualificação econômico-financeira.

4.1.1 Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.2 Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

4.3 Não poderão participar desta licitação os interessados:

4.3.1 proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.3.2 que não atendam às condições deste Edital e seu(s) anexo(s);

4.3.3 Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.3.4 Que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.3.5 que estejam sob falência, recuperação judicial ou extrajudicial, ou concurso de credores ou insolvência, em processo de dissolução ou liquidação, observado o disposto no item 9.10.1.1 deste

Edital;

4.3.6 Entidades empresariais que estejam reunidas em consórcio;

4.3.7 Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).

4.4 Como condição para participação no Pregão, a licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.4.1 que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

4.4.2 nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.4.2.1 nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

4.4.3 Que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.4.4 Que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.4.5 Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.4.6 Que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

4.4.7 Que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.4.8 que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.4.9 que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.4.10 que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência (em caso de fornecimento de bens de informática).

4.5 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1 Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

5.2 O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3 Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurando aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4 As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

5.5 Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

5.7 Não será estabelecida, nesta etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6 DO PREENCHIMENTO DA PROPOSTA

6.1 O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1 *Valor unitário e total do item;*

6.1.2 Marca;

6.1.3 Fabricante;

6.1.4 Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, *o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso;*

6.2 Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

6.4 Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.5 O prazo de validade da proposta não será inferior a 100 (cem) dias, a contar da data de sua apresentação.

6.6 O licitante deverá declarar, para cada item, em campo próprio do sistema COMPRASNET, se o produto ofertado é manufaturado nacional beneficiado por um dos critérios de margem de preferência indicados no Termo de Referência.

6.7 Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

6.8 O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a fiscalização do Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7 DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1 A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

7.2 O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

7.3 Também será desclassificada a proposta que identifique o licitante.

7.4 A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.4.1 A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.5 O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.6 O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.7 Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.7.1 O lance deverá ser ofertado pelo valor *unitário do item.*

7.8 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.9 O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

7.10 O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20)

segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo SISTEMA os respectivos lances.

7.10.1 *Será adotado para o envio de lances no pregão eletrônico o modo de disputa "aberto e fechado", em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.*

7.10.1.1 A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

7.10.1.2 Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

7.10.1.3 Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

7.10.1.4 Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.

7.10.1.5 *Não havendo lance final e fechado classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.*

7.10.1.6 Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender às exigências de habilitação.

7.11 Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia;

7.12 Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

7.13 Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.14 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.15 No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.16 Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

7.17 O critério de julgamento adotado será o menor preço, conforme definido neste Edital e seus

anexos.

7.18 Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.19 Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.20 Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

7.21 A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.22 Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.23 No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.24 Quando houver propostas beneficiadas com as margens de preferência em relação ao produto estrangeiro, o critério de desempate será aplicado exclusivamente entre as propostas que fizerem jus às margens de preferência, conforme regulamento.

7.25 A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.26 Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

7.26.1 no país;

7.26.2 por empresas brasileiras;

7.26.3 por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.26.4 por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.27 Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.28 Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

7.28.1 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.28.2 O pregoeiro solicitará ao licitante melhor classificado que, no prazo de XXX (XXX) horas [mínimo de duas horas], envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.29 Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7.30 **Para a aquisição de bens comuns de informática e automação,** definidos no art. 16-A da Lei n° 8.248, de 1991, será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

7.31 Nas contratações de bens e serviços de informática e automação, nos termos da Lei nº 8.248, de 1991, as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

7.32 Quando aplicada a margem de preferência a que se refere o Decreto nº 7.546, de 2 de agosto de 2011, não se aplicará o desempate previsto no Decreto nº 7.174, de 2010.

7.33 Para produtos abrangidos por **margem de preferência**, caso a proposta de menor preço não tenha por objeto produto manufaturado nacional, o sistema automaticamente indicará as propostas de produtos manufaturados nacionais que estão enquadradas dentro da referida margem, para fins de aceitação pelo Pregoeiro.

7.34 Nesta situação, a proposta beneficiada pela aplicação da margem de preferência tornar-se-á a proposta classificada em primeiro lugar.

8 DA ACEITABILIDADE DA PROPOSTA VENCEDORA

8.1 Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

8.2 O Pregoeiro solicitará ao licitante provisoriamente classificado em primeiro lugar que apresente ou envie juntamente com a proposta, sob pena de não-aceitação, certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012, conforme exigido no Termo de Referência.

8.3 O licitante qualificado como produtor rural pessoa física deverá incluir, na sua proposta, os

percentuais das contribuições previstas no art. 176 da Instrução Normativa RFB n. 971, de 2009, em razão do disposto no art. 184, inciso V, sob pena de desclassificação.]

8.4 Será desclassificada a proposta ou o lance vencedor, apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 – TCU – Plenário), ou que apresentar preço manifestamente inexequível.

8.5 Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.6 Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

8.7 Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

8.8 O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de 02h (duas horas) ou prazo definido pelo pregoeiro, sob pena de não aceitação da proposta.

8.8.1 O prazo estabelecido poderá ser prorrogado pelo Pregoeiro por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.

8.8.2 Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

8.9 Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.10 Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

8.11 O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

8.12 Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

8.13 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.14 Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte,

sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

8.15 Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9 DA HABILITAÇÃO

9.1 Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

9.1.1 SICAF;

9.1.2 Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/)

9.1.3 A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.1.3.1 Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

9.1.3.2 A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

9.1.3.3 O licitante será convocado para manifestação previamente à sua desclassificação.

9.1.4 Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.1.5 No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.2 Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1 O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;

9.2.2 É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a

apresentação da proposta, a respectiva documentação atualizada.

9.2.3 O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

9.3 Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo *mínimo de duas horas*, sob pena de inabilitação (a diligência em questão permite, apenas, a solicitação de documentos outros para confirmação dos já apresentados, sendo exemplo a requisição de cópia de contrato de prestação de serviços que tenha embasado a emissão de atestado de capacidade técnica já apresentado).

9.4 Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais **quando houver dúvida** em relação à integridade do documento digital.

9.5 Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

9.6 Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

9.6.1 Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7 Ressalvado o disposto no item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

9.8 Habilitação jurídica:

9.8.1 No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.8.2 Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual – CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

9.8.3 No caso de sociedade empresária ou empresa individual de responsabilidade limitada – EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

9.8.4 Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

9.8.5 No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

9.8.6 No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das

Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

9.8.7 No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

9.8.8 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

9.9 **Regularidade fiscal e trabalhista:**

9.9.1 Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

9.9.2 Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

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

9.9.5 Prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.6 Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.9.7 Caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

9.9.8 Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

9.10 **Qualificação Econômico-Financeira**.

9.10.1 Certidão negativa de falência, recuperação judicial ou recuperação extrajudicial expedida pelo
distribuidor da sede do licitante;

9.10.1.1 No caso de certidão positiva de recuperação judicial ou extrajudicial, o licitante deverá apresentar a comprovação de que o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n.º 11.101, de 09 de fevereiro de 2005, sob pena de inabilitação, devendo, ainda, comprovar os demais requisitos de habilitação.

9.10.2 Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.10.3 No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro. (Art. 3º do Decreto nº 8.538, de 2015);

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

9.10.3.2 É admissível o balanço intermediário, se decorrer de lei ou contrato social/estatuto social.

9.10.3.3 Caso o licitante seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

9.10.4 A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

9.10.5 As empresas que apresentarem resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar, considerados os riscos para a Administração, e, a critério da autoridade competente, o capital mínimo ou o patrimônio líquido mínimo de 10% (dez por cento) do valor estimado da contratação ou do item pertinente.

9.11 Qualificação Técnica

9.11.1 As empresas, cadastradas ou não no SICAF, deverão comprovar, ainda, a qualificação técnica, por meio de:

9.11.1.1 Atestados de Capacidade Técnica para comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

9.12 O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do

tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

9.13 A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

9.14 A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.15 Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.16 A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.17 Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

9.18 Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.19 Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.20 Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10 DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1 A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo mínimo de 02 (duas) horas, ou prazo definido pelo Pregoeiro, a contar da sua solicitação no sistema eletrônico e deverá:

10.1.1 Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2 Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2 A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.3 Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

10.4 Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

10.5 Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.6 A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.7 A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

10.8 As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação, no site https://www.comprasgovernamentais.gov.br/.

10.9 Deverá ser entregue junto com os documentos de habilitação planilha comprobatória das especificações técnicas item a item, contendo link para os referidos documentos do fabricante com informações sobre a especificação solicitada;

11 DOS RECURSOS

11.1 Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2 Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1 Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2 A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3 Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.2.4 O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.2.5 Os autos do processo permanecerão com vista franqueada aos interessados, no endereço

constante neste Edital.

12 DA REABERTURA DA SESSÃO PÚBLICA

12.1 A sessão pública poderá ser reaberta:

12.1.1 Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2 Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2 Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1 A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, ou, ainda, fac-símile, de acordo com a fase do procedimento licitatório.

12.2.2 A convocação feita por e-mail ou fac-símile dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13 DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1 O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2 Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14 DA GARANTIA DE EXECUÇÃO

14.1 Não haverá exigência de garantia de execução para a presente contratação.

15 DA ATA DE REGISTRO DE PREÇOS

15.1 Homologado o resultado da licitação, terá o adjudicatário o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2 Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no prazo de 05 (cinco) dias, a contar da data de seu recebimento.

15.3 O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o

seu transcurso, e desde que devidamente aceito.

15.4 Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

15.4.1 Será incluído na ata, sob a forma de anexo, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993;

15.5 O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

15.5.1 A referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

15.5.2 A contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

15.5.3 A contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

15.6 O prazo de vigência da contratação é de 12 meses.

15.7 Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

15.7.1 Nos casos em que houver necessidade de assinatura da Ata de Registro de Preços, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

15.7.2 Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

15.8 Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

15.9 Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

16 DO REAJUSTAMENTO, DO RECEBIMENTO DO OBJETO, DAS OBRIGAÇÕES E DO PAGAMENTO

16.1 As regras acerca do reajustamento em sentido geral do valor contratual, os critérios de recebimento e aceitação do objeto e de fiscalização, as obrigações da Contratante e da Contratada, e as regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

17 DAS SANÇÕES ADMINISTRATIVAS

17.1 Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

17.1.1 Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

17.1.2 Não assinar a ata de registro de preços, quando cabível;

17.1.3 Apresentar documentação falsa;

17.1.4 Deixar de entregar os documentos exigidos no certame;

17.1.5 Ensejar o retardamento da execução do objeto;

17.1.6 Não mantiver a proposta;

17.1.7 Cometer fraude fiscal;

17.1.8 Comportar-se de modo inidôneo;

17.2 As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

17.3 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

17.4 O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

17.4.1 Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

17.4.2 Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

17.4.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

17.4.4 Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

17.4.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

17.5 A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

17.6 Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, as cópias do processo administrativo que forem necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

17.7 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

17.8 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

17.9 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

17.10 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

17.11 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

17.12 As penalidades serão obrigatoriamente registradas no SICAF.

17.13 As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

18 DA FORMAÇÃO DO CADASTRO DE RESERVA

18.1 Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.

18.2 A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.

18.3 Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

18.4 Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos artigos 20 e 21 do Decreto n° 7.892/213.

19 DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

19.1 Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

19.2 A impugnação poderá ser realizada por forma eletrônica, pelo e-mail licitacoes@ifsc.edu.br, ou por petição dirigida ou protocolada no endereço da Reitoria do IFSC, Rua 14 de julho, 150 Enseada dos Marinheiros, Coqueiros, Florianópolis, SC – 88075-010.

19.3 Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até dois dias úteis contados da data de recebimento da impugnação.

19.4 Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

19.5 Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

19.6 O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

19.7 As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

19.8 A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

19.9 As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

20 DAS DISPOSIÇÕES GERAIS

20.1 Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

20.2 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

20.3 Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

20.4 No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

20.5 A homologação do resultado desta licitação não implicará direito à contratação.

20.6 As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

20.7 Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a

Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

20.8 Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

20.9 O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

20.10 Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

20.11 Os critérios de sustentabilidade adotados para essa aquisição são balizados pelo Guia Nacional de Licitações Sustentáveis e demais legislações pertinentes, e podem ser verificados diretamente nas descrições dos itens contidas no Quadro de Especificações Mínimas.

20.12 O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.comprasgovernamentais.gov.br/, www.ifsc.edu.br, e também poderão ser lidos e/ou obtidos no endereço da Reitoria do IFSC, Rua 14 de julho, 150 Enseada dos Marinheiros, Coqueiros, Fpolis, SC - 88075-010, nos dias úteis, no horário das 08:00 às 12:00 e das 13:00 às 17:00 horas, mediante prévio agendamento pelo e-mail licitacoes@ifsc.edu.br mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

20.13 Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Documento de Oficialização de Demanda;
ANEXO II – Estudo Técnico Preliminar;
ANEXO III – Termo de Referência;
ANEXO IV – Mapa de Gestão de Risco
ANEXO V – Minuta da Ata de Registro de Preços
ANEXO VI – Minuta de Autorização de Fornecimento (AF)
ANEXO VII – Declaração do Simples Nacional (conforme IN RFB 1.234, de 11 de janeiro de 2012.)
ANEXO VIII – Dados para Cadastramento da Empresa
ANEXO IX – Termo de Sigilo e Responsabilidade

Florianópolis, XX de XXXXXXX de 20XXXXX

NOME XXXXXXXX

Pró-Reitor de Administração do IFSC

350
IFSC
Fls.nº ____

ANEXO III
TERMO DE REFERÊNCIA

Processo Administrativo nº 23292.010214/2021-24

Histórico de Revisões

Data	Versão	Descrição	Autor
03/08/2021	1.0	Finalização da primeira versão do documento.	EPC
08/09/2021	1.1	Atualização de requisitos de sustentabilidade.	EPC

1 DO OBJETO

1.1 Aquisição de **SOLUÇÃO UNIFICADA DE SEGURANÇA E CONECTIVIDADE SEM FIO**, conforme condições, quantidades e exigências estabelecidas neste instrumento:

As descrições, quantidades e valores dos itens deste processo encontram-se no anexo intitulado Quadro de Especificações Mínimas.

AS QUANTIDADES QUE, PORVENTURA, FOREM ENTREGUES INCORRETAMENTE NO CAMPUS OU FALTANDO PARTE DA AF SERÃO DEVOLVIDAS E OS CUSTOS COBERTOS PELA LICITANTE VENCEDORA.

1.2 O prazo de vigência da contratação é de 12 meses contados do(a) data de início da Ata de Registro de Preços na forma do art. 12, do Dec n° 7.892/13.

2 JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1 O Instituto Federal de Santa Catarina, visando suprir possíveis demandas no exercício de suas atividades, realiza licitações através do Sistema de Registro de Preços. Essas licitações são feitas de forma compartilhada, ou seja, atendendo todos os Câmpus no Estado de Santa Catarina. Atualmente participam das licitações os Campus Araranguá, Caçador, Canoinhas, Cerfead, Chapecó, Criciúma, Florianópolis, Florianópolis – Continente, Garopaba, Gaspar, Itajaí, Jaraguá do Sul – Centro, Jaraguá do Sul – Rau, Joinville, Lages, Palhoça, Reitoria, São Carlos, São José, São Lourenço do Oeste, São Miguel do Oeste, Tubarão, Urupema e Xanxerê.

2.2 A finalidade do IFSC é formar e qualificar profissionais no âmbito da educação profissional e tecnológica, nos diferentes níveis e modalidades de ensino, para os diversos setores da economia, bem como realizar pesquisa aplicada e promover o desenvolvimento tecnológico de novos processos, produtos e serviços, em estreita articulação com os setores produtivos e a sociedade, especialmente de abrangência local e regional, oferecendo mecanismos para a educação continuada. Neste sentido, a presente licitação tem como objetivo garantir celeridade e eficiência no momento da aquisição, garantindo a qualidade nos serviços prestados ao cidadão.

2.3 A modalidade de licitação definida neste processo cumpre o disposto nos Decretos nº 5.450/2005 e 7.892/2013, permitindo assim a aquisição de forma parcelada, nas quantidades e no momento adequado

351
IFSC
Fls.nº ____

às necessidades do IFSC.

2.4 A eventual aquisição da solução ora apresentada justifica-se pela obsolescência da solução atual de conectividade sem fio implantada no IFSC bem como pelas soluções individuais de segurança (firewall) implantadas nos Câmpus como apresentado no Estudo Técnico Preliminar. Considera-se ainda que houve interesse de contratação da solução de firewall iniciada no Estudo Técnico Preliminar que resultou no PE 118/2020 mas não concretizada naquele momento.

3 REQUISITOS DE CONTRATAÇÃO

- Identificação das necessidades de negócio: Permitir que sistemas de gestão e acadêmico, portais e aplicativos sejam acessados facilmente pelos usuários a partir de seus dispositivos móveis e que a transmissão dos dados ocorra de forma segura pela rede de dados institucional.
- Identificação das necessidades tecnológicas: Renovação tecnológica considerando os pontos levantados no item 1 e pela necessidade de renovação das aplicações de firewall.
- Requisitos Ambientais: Atendimento à legislação ambiental brasileira para produção e descarte de materiais.
    - Para os itens 23 a 26 (nobreaks), durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008.
- Requisitos Legais: A contratação deverá estar em conformidade com a legislação que rege os processos de contratação no setor público (Lei 8.666/93, Lei 10.520/02, Lei 14.133/21, suas alterações e regulamentações);
- Adequação do ambiente para execução contratual: O objeto deste processo consiste na substituição e expansão de solução que já está implantada na instituição e que por isso não necessita de adequação do ambiente físico ou lógico para sua execução.
- Requisitos de Capacitação: A empresa contratada deverá prestar treinamento para os técnicos de TIC do IFSC que farão o gerenciamento da solução.
- Requisitos de Logística: A empresa vencedora deverá entregar todos os equipamentos nos endereços listados no edital dentro do prazo de entrega estabelecido no mesmo;
- Requisitos de Segurança: O acesso ao ambiente físico/lógico deverá ser realizado com supervisão de um técnico de TIC e de forma limitada ao escopo do projeto.
- Requisitos de Suporte: A empresa vencedora deverá prestar garantia para todos os equipamentos adquiridos de acordo com as especificações do edital, obedecendo forma e prazo de atendimento/solução; e/ou suportar os serviços contratados.

4 ACORDO DE NÍVEL DE SERVIÇO (SLA) E GARANTIAS

4.1 SLA

4.1.1 Primeiro atendimento em até 30 minutos após abertura de chamado;

4.1.2 A empresa contratada terá até 15 dias corridos para identificar o problema e encaminhar a resolução do mesmo;

4.1.3 Prazo de resolução de problemas de hardware: envio do equipamento substituto no próximo dia útil;

4.1.4 O IFSC pode, a qualquer momento, solicitar atendimento *onsite* para casos complexos, centralizando as demandas de atendimento na reitoria em Florianópolis/SC;

352
IFSC
Fls.nº ____

4.2 **Garantia e Suporte**

4.2.1 Garantia: Mínimo de 03 anos oficial do fabricante. Deve ser apresentado portal do fabricante com a relação dos *seriais numbers* e vigência do contrato;

4.2.2 Suporte: Cumulativamente por telefone 0800, e-mail e portal de helpdesk/servicedesk com login/senha próprio para o IFSC. Todos os chamados devem ser registrados no portal para consulta histórica. Deve ser possível que o IFSC faça a consulta do histórico dos chamados diretamente no portal a qualquer momento;

4.2.3 Manutenção: Não será aceito o conserto de equipamentos que apresentarem problemas de hardware. A empresa vencedora deverá trocar os mesmos por equipamentos novos;

5 **CONDIÇÕES GERAIS DA CONTRATAÇÃO**

5.1 Condições de Participação e Realização dos Serviços

- A solução deverá ser constituída dos equipamentos e ferramentas relacionadas nos itens deste grupo (lote), garantindo a entrega por uma única empresa e a total compatibilidade entre eles;
- A licitante deverá apresentar, com a sua proposta comercial, uma planilha “ponto a ponto”, indicando a documentação do fabricante (datasheets, especificações técnicas, manual do produto, sítio web do próprio fabricante, etc.), que comprovem o atendimento de todos os requisitos técnicos acima exigidos neste Termo de Referência

5.2 Condições de Aceite

- 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;
- O IFSC poderá efetuar consulta do número de série do equipamento, junto ao fabricante, informando data de compra e empresa adquirente, confirmando a procedência legal dos equipamentos;
- O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;

6 CLASSIFICAÇÃO DOS BENS COMUNS

6.1 Os objetos em aquisição nesta licitação tratam-se de bens de natureza comuns tipificada na Lei nº 10.520/2002 cujos padrões de desempenho e qualidade são objetivamente definidos por este Termo de Referência, por meio de especificações usuais no mercado.

7 **ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO**

7.1 O prazo de entrega dos bens é de 45 (quarenta e cinco) dias corridos para produtos produzidos no Brasil e 90 (noventa) dias corridos para produtos produzidos fora do Brasil (importados) após o envio de uma **Autorização de Fornecimento (AF)** pela Administração, somente por e-mail, nos seguintes endereços:

CÂMPUS	ENDEREÇO
Câmpus Araranguá	Av. XV de Novembro, s/nº – Bairro Aeroporto – CEP: 88900-000 – Araranguá – SC – Fone: (48) 3311-5000; e-mail: compras.ararangua@ifsc.edu.br.
Câmpus Caçador	Av. Fahdo Thomé, 3000, Champagnat – Caçador – SC – 89500-000, Fone: (49) 3561-5700; e-mail: compras.cdr@ifsc.edu.br.
Câmpus Canoinhas	AV. Expedicionários, 2150 – Bairro Campo do Água Verde – CEP 89460-000 –

353
IFSC
Fls.nº ____

	Canoinhas SC: Fone: (47) 3627- 4500; e-mail: compras.canoinhas@ifsc.edu.br.
Cerfead	Rua Duarte Schutel, 99 – Centro – Florianópolis/SC – CEP 88015- 640; Fone: (48) 3131-8816; e-mail: compras@ifsc.edu.br;
Câmpus Chapecó	Av. Nereu Ramos, 3450 D – Bairro Seminário – Chapecó/SC – CEP: 89813-000 – Fone: (49) 3313-1240; e-mail:compras.chapeco@ifsc.edu.br.
Câmpus Criciúma	SC 443, km 01, nº. 845 - Bairro Vila Rica – Criciúma – SC – CEP 88813-600; Esquina com Rua Antônio Daré; Fone: (48) 3462-5000; e-mail: compras.criciuma@ifsc.edu.br.
Câmpus Florianópolis	Av. Mauro Ramos, 950 – Centro – Florianópolis/SC. CEP: 88020-300; Almoxarifado; Fone: (48) 3211-6000; e-mail: compras.fpolis@ifsc.edu.br.
Câmpus Florianópolis Continente	Rua 14 de Julho, 150 – Coqueiros - Florianópolis/SC – CEP: 88.075- 010; Fone (48) 3877-8400; e-mail: compras.continente@ifsc.edu.br.
Câmpus Garopaba	Rua Maria Aparecida Barbosa, nº 153, Loteamento Vila de Campo - Bairro Campo Duna – Garopaba - SC – CEP 88495-000; Fone (48) 3254-7330; e-mail: compras.garopaba@ifsc.edu.br.
Câmpus Gaspar	Rua Adriano Kormann, 510 – Bairro Bela Vista – Gaspar – SC; CEP 89110-971; Fone: (47) 3318-3700; e-mail:compras.gaspar@ifsc.edu.br.
Câmpus Itajaí	Av. Vereador Abrahão João Francisco, 3899, Bairro Ressacada – Itajaí – SC; CEP 88307-303; Fone: (47) 3390-1200; e-mail: compras.itj@ifsc.edu.br.
Câmpus Jaraguá do Sul – Rau	Rua dos Imigrantes, nº 445 – Bairro Rau – 89254-430 – Jaraguá do Sul; Fone: (47) 3276-9600; e-mail: compras.gw@ifsc.edu.br
Câmpus Jaraguá do Sul	Av. Getúlio Vargas, nº 830 – Centro – Jaraguá do Sul – CEP: 89251- 000, Fone: (47) 3276-8700; e-mail: compras.jar@ifsc.edu.br.
Câmpus Joinville	Rua Pavão, 1337 – Loteamento Novo Horizonte – Bairro Costa e Silva, Joinville/SC – CEP: 89220-618 – Fone: (47) 3431-5600; e-mail: compras.joinville@ifsc.edu.br.
Câmpus Lages	Rua Heitor Vila Lobos, s/n – Bairro São Francisco – Lages – CEP 88506-400, Fone: (49) 3221-4200; e-mail: compras.lages@ifsc.edu.br.
Câmpus Palhoça-Bilíngue	Rua João Bernardino da Rosa – Bairro Cidade Universitária Pedra Branca – Palhoça – SC – CEP 88137-010; Fone: (48) 3341-9700; e mail: compras.phb@ifsc.edu.br.
Câmpus São Carlos	Rua Aloisio Stoffell, 1271 – Jardim Alvorada – São Carlos/SC – CEP 89885-000; Fone: (49) 3325-4149; e-mail: compras.sca@ifsc.edu.br
Câmpus São José	R. José Lino Kretzer, 608 – Bairro Praia CompridaSão José – SC – CEP: 88103-310; Fones: (48) 3381-2800 e Fax: 3381-2812; e-mail: compras.sje@ifsc.edu.br
Câmpus São Lourenço do Oeste	Rua Aderbal Ramos da Silva, 496-514 - Bairro Progresso. São Lourenço do Oeste – CEP 89990 000; Fones: (049) 3344-8495; e mail: compras.slo@ifsc.edu.br.
Câmpus São Miguel do Oeste	Rua 22 de Abril, s/n – Bairro São Luiz – São Miguel do Oeste – SC 89900-970, Fone: (49)3631-0400; e-mail: compras.smo@ifsc.edu.br.
Câmpus Tubarão	Rua Deputado Olices Pedra de Caldas, 480, Dehon, Tubarão / SC - CEP 88704-296; Fone: (48) 3301-9101; e-mail: compras.tub@ifsc.edu.br
Câmpus Urupema	Estrada do Senadinho s/n – Centro – Urupema – SC – 88625-970, Fone: (49) 3236-3100; e-mail: compras.urupema@ifsc.edu.br.

Câmpus Xanxerê	Rua Euclides Hack, 1603 – Bairro Veneza – Xanxerê – SC – 89820- 000; Fone: (49) 3441-7900; e-mail: compras.xxe@ifsc.edu.br.
Reitoria	Av. 14 de julho 150 – Coqueiros – Florianópolis – SC – CEP:88075- 010 – Fones: (48) 3877-9000; e-mail: compras@ifsc.edu.br.

7.2 Os bens serão recebidos provisoriamente no momento de sua entrega, por servidor(a) do IFSC devidamente identificado, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.
7.3 Os bens serão recebidos provisoriamente no prazo de 15 (quinze) dias, pelo(a) responsável pelo recebimento para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.4 Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.5 Os bens serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

7.5.1 Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

7.6 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

7.7 A contratada se obriga a entregar todo o material, no mesmo momento, na quantidade informada na Autorização de Fornecimento (AF). Somente poderá ser aceita a entrega parcial, nas hipóteses abaixo, sob pena de devolução de todo material, no caso do empenho/AF não estar completa:

7.7.1 O material só poderá ser entregue parcialmente, se a licitante encaminhar justificativa, solicitando o cancelamento dos itens pendentes juntamente ao material, para ser avaliada pela Administração e posterior aplicação de penalidades;

7.7.2 A Administração poderá solicitar a antecipação da entrega de parte dos materiais constantes da Autorização de Fornecimento, somente se a licitante conseguir atender ao pedido.

8 OBRIGAÇÕES DA CONTRATANTE

8.1 São obrigações da Contratante:

8.1.1 Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

8.1.2 Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

8.1.3 Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

8.1.4 Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

8.1.5 Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

8.2 A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

9 OBRIGAÇÕES DA CONTRATADA

9.1 A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

9.1.1 Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Subitem 7.1 deste Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

9.1.1.1 O objeto deve estar acompanhado do manual do usuário, com uma versão em português ou inglês e da relação da rede de assistência técnica autorizada;

9.1.2 Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

9.1.3 Substituir, reparar ou corrigir, às suas expensas, no prazo de 05 (cinco) dias úteis, o objeto com avarias ou defeitos;

9.1.4 Materiais entregues em desacordo com o Edital e não retirados em até 05 (cinco) dias úteis após comunicação formal do IFSC, serão descartadas. Este prazo poderá ser prorrogado, desde que formalizado, justificado e aceito pelo IFSC. Esta prorrogação somente será aceita caso seja feita dentro do prazo da notificação.

9.1.5 Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.1.6 Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.1.7 Responder pelas perdas e danos causados por seus empregados, durante o fornecimento do material, ainda que involuntariamente, às instalações do prédio, máquinas, equipamentos e demais bens do IFSC, substituindo os referidos bens por outros semelhantes em prazo que lhe será expressamente combinado pela Contratante.

9.1.8 Todos os itens constantes da nota de empenho devem ser entregues no mesmo momento, nas condições e locais conforme consta deste Anexo **(não será aceita a entrega parcelada dos itens).**

9.1.9 Retirar a nota de empenho em até 03 (três) dias úteis, após a convocação.

9.1.10 Cumprir o prazo de garantia de acordo com o especificado em cada item neste Termo de Referência ou conforme o prazo estabelecido na proposta de preços, caso este seja maior que o mínimo estabelecido.

9.1.11 Os problemas apresentados durante o prazo de garantia devem ser solucionados em até 30 (trinta) dias corridos.

9.1.12 Arcar com todos os custos para cumprimento da garantia, inclusive no caso de necessidade de transporte (técnicos ou equipamentos).

9.1.13 A Contratada assume o compromisso de receber as **Autorizações de Fornecimento (AF's)** e Empenhos pelo e-mail institucional informado na **DECLARAÇÃO DE CONCORDÂNCIA À ATA DE REGISTRO DE PREÇOS c**oncordando que não sendo confirmado o recebimento do e-mail, o IFSC considerará como recebido, iniciando a contagem do prazo de entrega. Assumindo o compromisso de

356
IFSC
Fls.nº ____

avisar o IFSC quando houver mudança do e-mail.

9.1.14 **Manter atualizado seu cadastro no órgão através do envio do documento preenchido referente ao Anexo VIII deste edital sempre que houver mudanças em seus dados cadastrais.**

9.1.15 O representante da Contratada deverá assinar o Termo de Sigilo e Responsabilidade disponível no **Anexo IX** deste edital.

10 DA SUBCONTRATAÇÃO

10.1 Não será admitida a subcontratação do objeto licitatório.

11 DA ALTERAÇÃO SUBJETIVA

11.1 É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

12 DO PAGAMENTO

12.1 O pagamento deverá ser efetuado integral até o 15º (décimo quinto) dia útil após o aceite definitivo do material, em sua totalidade, e atesto da Nota Fiscal ou Documento de Cobrança, através de ordem bancária, para crédito em banco, com o código da agência e o número da conta-corrente que forem indicados pelo contratado.

12.1.1 Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

12.2 Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

12.3 A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

12.3.1 Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

12.4 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

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

12.6 Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

12.7 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

12.8 Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar

357
IFSC
Fls.nº ____

consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

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

12.10 Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

12.11 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

12.11.1 Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

12.12 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

12.12.1 A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

12.13 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento; VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX)$$

$$\frac{(6/100)}{365}$$

I = 0,00016438

TX = Percentual da taxa anual = 6%

12.14 A Nota fiscal/fatura ou documento de cobrança deverá ser sempre emitida com o CNPJ do Câmpus requisitante, conforme descrição abaixo:

CÂMPUS	CNPJ
Araranguá	11.402.887/0008-37
Caçador	11.402.887/0018-09
Canoinhas	11.402.887/0012-13
Chapecó	11.402.887/0007-56
Continente	11.402.887/0004-03
Criciúma	11.402.887/0009-18
Florianópolis	11.402.887/0002-41
Garopaba	11.402.887/0021-04
Gaspar	11.402.887/0010-51
Geraldo Werninghaus	11.402.887/0019-90
Itajaí	11.402.887/0013-02
Jaraguá do Sul	11.402.887/0005-94
Joinville	11.402.887/0006-75
Lages	11.402.887/0011-32
Palhoça Bilíngue	11.402.887/0015-66
Reitoria	11.402.887/0001-60
São José	11.402.887/0003-22
São Miguel do Oeste	11.402.887/0014-85
Tubarão	11.402.887/0020-23
Urupema	11.402.887/0016-47
Xanxerê	11.402.887/0017-28

Para o Câmpus Avançado de São Lourenço do Oeste, a Nota Fiscal deverá ser emitida no CNPJ do Câmpus São Miguel, sendo os materiais entregues no respectivo Câmpus Avançado.

12.15 Poderá haver a emissão de mais de uma Nota fiscal/fatura ou documento de cobrança para cada Nota de Empenho ou apenas uma Nota fiscal/fatura ou documento de cobrança e, para acompanhar as mercadorias para os Câmpus, notas de remessa de materiais, aceitas pela fiscalização estadual.

13 **DO REAJUSTE**

13.1 Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

13.1.1 Fica ressalvada a possibilidade de Alteração das condições para a concessão de reajuste em

359
IFSC
Fls.nº ____

face da superveniência de normas federais aplicáveis à espécie.

14 ESTIMATIVAS DE PREÇOS DA CONTRATAÇÃO

14.1 O IFSC utiliza sistema próprio para realização de processos licitatórios denominado SIPAC – Sistema Integrado de Patrimônio, Administração e Contratos. Neste sistema são cadastradas as cotações fornecidas por empresas, conseguidas em pesquisa na Internet e/ou Painel de Preços.

14.2 Neste processo estão elencadas cotações conseguidas através de fornecedores e/ou Painel de Preços. As cotações foram disponibilizadas no ETP e a média linear simples foi cadastrada no SIPAC para validação interna do processo.

15 ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

15.1 Fonte de Recursos:

15.1.1 Orçamento das unidades (2021) [1]

15.1.1.1 Custeio: R$ 45.289.930,00

15.1.1.2 Investimento: R$ 1.044.085,00

15.2 Estimativa de Impacto Econômico-Financeiro

15.2.1 Exercício 2021/2022

15.2.1.1 Valor final estimado para Custeio: R$ 393.311,87

15.2.1.1.1 Percentual do recurso em Custeio: 0,87%

15.2.1.2 Valor final estimado para Investimento: R$ 4.025.105,41

15.2.1.2.1 Percentual do recurso em Investimento: 385,5%

[1] Fonte: INSTRUÇÃO NORMATIVA Nº 13, DE 12 DE MAIO DE 2021 (Retifica a IN 29/2020 que Dispõe sobre a revisão do Plano Anual de Trabalho 2021 do Instituto Federal de Santa Catarina – IFSC)

16 DA GARANTIA DE EXECUÇÃO

16.1 Não haverá exigência de garantia contratual da execução.

17 DAS SANÇÕES ADMINISTRATIVAS

17.1 Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

17.1.1 Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

17.1.2 Ensejar o retardamento da execução do objeto;

17.1.3 Falhar ou fraudar na execução do contrato;

17.1.4 Comportar-se de modo inidôneo;

17.1.5 Cometer fraude fiscal;

17.2 Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

360
IFSC
Fls.nº ____

17.2.1 **Advertência,** por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

17.2.2 multas (que deverão ser recolhidas em favor do Instituto Federal de Educação, Ciências e Tecnologia de Santa Catarina, a ser preenchido de acordo com instruções fornecidas pela Contratante):

17.2.2.1 de 1% (um por cento) sobre o valor total do somatório dos itens entregues com atraso (AF), por dia de atraso na entrega do material, limitados a 10%(dez por cento) do mesmo valor.

17.2.2.2 de 10% (dez por cento) sobre o valor total da Autorização de Fornecimento (AF), por infração a qualquer cláusula ou condição do Edital, não especificada na alínea “a” deste inciso, aplicada em dobro na reincidência.

17.2.2.3 de 10% (dez por cento) sobre o valor total da Proposta de preços vencedora, no caso de recusa injustificada da licitante adjudicatária em assinar a Ata de Registro de Preço ou deixar de apresentar os documentos exigidos, nos prazos e condições estabelecidas neste Edital.

17.2.2.4 de 10% (dez por cento) sobre o valor total da Proposta de preço, no caso de rescisão do contrato por ato unilateral da administração, motivado por culpa da Contratada, garantida prévia defesa, independente das demais sanções cabíveis;

17.2.2.5 de 10% (dez por cento) sobre o valor total do somatório dos itens entregues em desacordo, por apresentação de marca e/ou modelo que não estão de acordo com a especificação do edital e apresentada na proposta de preço da licitante;

17.2.2.6 de 10% (dez por cento) do valor total do somatório dos itens entregues em desacordo com o Edital e a proposta de preços aceita na sessão do pregão;

17.2.2.7 de 0,5% (cinco décimos por cento) ao dia sobre o valor adjudicado, no caso de não substituição do material no prazo determinado no Termo de Referência, caso não estaria de acordo com a especificação exigida em Edital, limitada a incidência a 10 (dez) dias úteis. Após o décimo dia e a critério da Administração, poderá ocorrer a não-aceitação do material e/ou a sua substituição, de forma a configurar, nessa hipótese inexecução parcial da obrigação assumida;

17.2.2.8 de 10% (dez por cento) sobre o valor total da Ata de Registro de Preços, no caso de cancelamento integral da ata por ato unilateral da administração, motivada por culpa da Contratada ou a pedido da mesma;

17.2.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

17.2.4 Impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

17.2.4.1 A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 19.1 deste Termo de Referência.

17.2.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

17.3 As sanções previstas nos subitens acima poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

17.4 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

361
IFSC
Fls.nº ____

17.4.1 Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

17.4.2 Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

17.4.3 Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

17.5 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

17.6 As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

17.7 Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de XX (XXXX) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

17.8 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

17.9 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

17.10 Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

17.11 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

17.12 As penalidades serão obrigatoriamente registradas no SICAF.

362
IFSC
Fls.nº ____

A Equipe de Planejamento da Contratação foi instituída pela Portaria no 798, de 12 de março de 2021.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
gov.br Documento assinado digitalmente Kari de Souza Soares Data: 08/09/2021 10:31:01-0300 Verifique em https://verificador.iti.br	gov.br Documento assinado digitalmente Benoni de Oliveira Pires Data: 08/09/2021 10:00:59-0300 Verifique em https://verificador.iti.br
INTEGRANTE ADMINISTRATIVO	

Pró-Reitora de Administração do IFSC

INSTITUTO FEDERAL DE SANTA CATARINA
SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS
EMITIDO EM 08/09/2021 08:33

QUADRO DE ESPECIFICAÇÕES MÍNIMAS

Licitação: 23292.010214/2021-24 - PE 32/2021 - REI
Assunto: AQUISIÇÃO DE SOLUÇÃO UNIFICADA DE SEGURANÇA E CONECTIVIDADE SEM FIO

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
NÃO ASSOCIADO(S) A LOTE/GRUPO					
23	NOBREAK 10 KVA - TORRE Características mínimas: Potência →10 kVA /10 kW; Tensão entrada → 115/220V~ (Bivolt); Tensão saída → 110/220V (De acordo com a solicitação de cada Câmpus indicada em AF); Fator de potência de saída →1; Conexão de entrada → bornes; Conexão de saída → Bornes + 8 tomadas NBR 14136 (20A); Formato → Torre; Transformador → Isolador; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Tempo de autonomia → 20 minutos no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008.	UNIDADE	10	19.222,04	192.220,40
24	NOBREAK 3KVA - RACK Características mínimas: Potência →3 kVA / 2,7 kW; Tensão entrada → 220V; Tensão saída → 220V; Fator de potência de saída → 0,9 ou superior; Conexão de entrada → Plugue NBR 14136 (20A); Conexão de saída → 6 tomadas NBR 14136 (20A); Formato → Rack (2U); Fusível →Rearmável; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Tempo de autonomia → 20 min, no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008.	UNIDADE	10	7.267,87	72.678,70

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
25	NOBREAK 3KVA - TORRE Características mínimas: Potência →3 kVA / 2,7 kW; Tensão entrada → 115/220V~ (Bivolt); Tensão saída → 110/220V (De acordo com a solicitação de cada Câmpus indicada em AF); Fator de potência de saída → 0,9 ou superior; Conexão de entrada → Plugue NBR 14136 (20A) + bornes; Conexão de saída → Bornes + 8 tomadas NBR 14136 (20A); Formato → Torre; Transformador → Isolador; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Fusível →Rearmável; Tempo de autonomia → 20 min, no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008.	UNIDADE	10	5.014,20	50.142,00
26	NOBREAK 6KVA - TORRE Características mínimas: Potência →6 kVA /6 kW; Tensão entrada → 115/220V~ (Bivolt); Tensão saída → 110/220V (De acordo com a solicitação de cada Câmpus indicada em AF); Fator de potência de saída →1; Conexão de entrada → bornes; Conexão de saída → Bornes + 8 tomadas NBR 14136 (20A); Formato → Torre; Transformador → Isolador; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia →Nobreak (UPS) online monofásico; Forma de Onda →Senoidal pura; Tempo de autonomia → 20 min, no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias – 1 ano; Disjuntor; Autoteste; - Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.**********Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA n° 401, de 04/11/2008.	UNIDADE	10	11.752,79	117.527,90
LOTE/GRUPO 1: SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA					
1	SWITCH TIPO 2 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA ---> Características Mínimas: 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo); 6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 7. Deve possuir tabela MAC com suporte a 8.000 endereços; 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 10. Deve suportar a comutação de Jumbo Frames; 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 10.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 14. Deve implementar serviço de DHCP Relay; 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela; 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 19. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um	UNIDADE	15	5.309,70	79.645,50

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 27. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 31. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 34. Deve suportar MAC Authentication Bypass (MAB); 35. Deve implementar RADIUS CoA (Change of Authorization); 36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 37. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 39. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 42. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 43. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 44. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 46. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 51. Deve permitir ser gerenciado através de IPv6; 52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 54. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 58. Deverá suportar ser configurado e monitorado através de REST API; 59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 60. Deve suportar temperatura de operação de até 45º Celsius; 61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 62. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 64. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
2	SWITCH TIPO 3 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com	UNIDADE	15	10.544,84	158.172,60

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 180W; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 8.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 28. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
3	Switch Tipo 4 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W a serem alocados em qualquer uma das portas 1000Base-T; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 8.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);	UNIDADE	15	13.130,96	196.964,40

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	28. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
4	SWITCH TIPO 5 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir capacidade de comutação de pelo menos 104 Gbps e ser capaz de encaminhar até 150 Mpps (milhões de pacotes por segundo); 6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 7. Deve possuir tabela MAC com suporte a 16.000 endereços; 8. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 9. Deve permitir a configuração de links agrupados virtualmente (link	UNIDADE	15	10.260,85	153.912,75

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 10. Deve suportar a comutação de Jumbo Frames; 11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 14. Deve implementar serviço de DHCP Relay; 15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 18. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 19. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 20. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 21. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 22. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 23. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 24. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 27. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 31. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 34. Deve suportar MAC Authentication Bypass (MAB); 35. Deve implementar RADIUS CoA (Change of Authorization); 36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 37. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 39. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 42. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 43. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 44. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 46. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 51. Deve permitir ser gerenciado através de IPv6; 52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 54. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 58. Deverá suportar ser configurado e monitorado através de REST API;				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 60. Deve suportar temperatura de operação de até 45º Celsius; 61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 62. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 64. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
5	SWITCH TIPO 6 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 104 Gbps e ser capaz de encaminhar até 150 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 16.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 15. Deve implementar serviço de DHCP Relay; 16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); 18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 19. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 20. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 22. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 23. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 24. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 25. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 28. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 35. Deve suportar MAC Authentication Bypass (MAB); 36. Deve implementar RADIUS CoA (Change of Authorization); 37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não	UNIDADE	15	14.826,84	222.402,60

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	causar indisponibilidade da rede; 39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio; 47. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 52. Deve permitir ser gerenciado através de IPv6; 53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch; 58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
6	TRANSCEIVER 1000BASE-SX 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 1000BASE-SX para fibras ópticas de até 400 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	UNIDADE	20	709,61	14.192,20
7	TRANSCEIVER 1000BASE-LX 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 1000BASE-X para fibras ópticas de até 10 kilometros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	UNIDADE	20	1.300,32	26.006,40
8	TRANSCEIVER 10GBASE-SR 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de até 300 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	UNIDADE	20	1.573,70	31.474,00

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
9	TRANSCEIVER 10GBASE-LR 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas de até 10 kilometros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	UNIDADE	20	1.364,37	27.287,40
10	FERRAMENTA DE GERENCIAMENTO CENTRALIZADO – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede dos campus e que garanta suporte a processos relativos à LGPD; 2. Deverá ser totalmente compatível com a solução proposta para gerenciamento da segurança e infraestrutura de rede dos campus; 3. A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato; 4. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 5. A solução deverá ser composta por elemento ou elementos fornecido(s) na forma de appliance virtual (máquina virtual) compatível com Vmware ESXi, Microsoft Hyper-V ou Linux KVM; 6. A solução deverá garantir a integridade da configuração de um determinado item através de bloqueio de alterações quando ocorrer acesso simultâneo de dois ou mais administradores no mesmo ativo; 7. A solução deverá possibilitar a criação e administração de políticas de firewall, controle de aplicação e filtro de URL; 8. A solução deverá permitir criar, de forma centralizada, novos objetos que poderão ser utilizados nas políticas; 9. A solução deverá permitir que o administrador localize em quais regras um determinado objeto (ex: computador, serviço, etc.) está sendo utilizado; 10. A solução deverá atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS; 11. A solução deverá permitir a criação de regras de filtragem de tráfego que fiquem ativas apenas em horários pré-definidos; 12. A solução deverá permitir a criação de regras de filtragem de tráfego com data de expiração; 13. A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso; 14. A solução deve permitir a criação de templates de configuração de túneis VPN IPSec a serem aplicados de maneira centralizada e padronizada em elementos concentradores VPN; 15. A solução deve permitir agendamento para a execução de configurações nos elementos administrados; 16. A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada; 17. A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches; 18. As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID; 19. As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso; 20. As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de wIDS ou wIPS; 21. As seguintes características de Bluetooth Low Energy (BLE) devem ser configuradas nos pontos de acesso através dos templates: configuração do UUID, Major ID, Minor ID, Beacon Interval e potência; 22. As seguintes características de VLAN devem ser configuradas nos switches através dos templates: VLAN, VLAN ID e endereçamento IP; 23. As seguintes características de segurança devem ser configuradas nos switches através dos templates: Autenticação 802.1X, Autenticação MAB e Guest VLAN; 24. As seguintes características de rede devem ser configuradas nos switches através dos templates: configuração das portas com respectivas VLANs tagged e untagged, configuração do protocolo LLDP e configurações de QoS; 25. A solução deve permitir que o administrador selecione em quais elementos os templates de configuração deverão ser aplicados; 26. A solução deve listar os elementos adminstrados e seu status de operação; 27. A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID; 28. A solução deve listar todos os Rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP; 29. A solução deve incorporar mapa mundi para visão unificada do status de operação dos elementos. Deve ainda permitir a adição de planta baixa de múltiplas localidades; 30. A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches; 31. A solução deve apresentar a topologia da rede com status dos elementos e informações sobre a atuação do protocolo Spanning-Tree em interfaces; 32. A solução deve permitir a execução de testes remotos para identificação de problemas em cabos de rede conectados aos switches; 33. A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração; 34. A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente; 35. A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas; 36. A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada; 37. A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada; 38. A solução deve permitir criar políticas/templates que	LICENÇA	2	59.405,80	118.811,60

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	definam a versão de firmware a ser distribuída e instalada em elementos administrados. Deve permitir ainda que o administrador da rede agende a atualização da versão de firmware de maneira automática nos elementos administrados; 39. A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio; 40. A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos; 41. A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos; 42. A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados; 43. A solução deve garantir visão centralizada das estatísticas de uso dos túneis VPN, com informações sobre volume de dados trafegados, horário da conexão e identificação do usuário que conectou na VPN; 44. A solução deverá ser capaz de receber os logs dos elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede das unidades e apresenta-los de forma centralizada; 45. A solução deverá ser capaz de receber, no mínimo, 5GB de logs diários; 46. A solução deverá ser capaz de armazenar, no mínimo, 3TB de informação; 47. A solução deverá ser capaz de armazenar os logs por 12 meses; 48. A solução deverá possuir mecanismo para que logs antigos sejam removidos automaticamente; 49. A solução deverá permitir a exportação dos logs; 50. A solução deverá permitir que o administrador realize download de um determinado conjunto de logs em formato texto ou CSV; 51. A solução deverá garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego; 52. A solução deverá permitir a extração de relatórios; 53. A solução deverá possuir relatórios pré-definidos; 54. A solução deverá possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida; 55. A solução deverá permitir a personalização de capas para os relatóri 56. A solução deverá permitir a geração de relatórios de logs de tráfego de dados; 57. A solução deverá permitir a personalização dos relatórios para inserção de gráficos dos tipos barra, linha, tabela e pizza; 58. A solução deverá possibilitar o envio de relatórios por e-mail de maneira automática; 59. A solução deverá permitir a customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da contratante, adaptando-o às suas necessidades; 60. A solução deverá permitir a definição de filtros nos relatórios; 61. A solução deverá ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros; 62. A solução deverá garantir a capacidade de criar consultas avançadas em sua base de dados que para as informações sejam utilizadas em gráficos e tabelas dentro dos relatórios; 63. A solução deverá implementar autenticação administrativa através do protocolos RADIUS ou TACACS; 64. A solução deverá permitir a criação de múltiplos perfis de usuários administradores com permissões granulares para limitar o acesso a determinadas funções e garantir privilégios de somente leitura e/ou leitura-escrita a outras; 65. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7. Durante o período de garantia deve ser possível a atualização do software para novas versões.				
11	UNIDADE DE SERVIÇO TÉCNICO PARA SITE SURVEY 1. O serviço de Site Survey será utilizado para análise técnica do ambiente real dos campus do IFSC em todas as localidades do estado de Santa Catarina de forma presencial nos respectivos endereços, apoiada por ferramentas e softwares adequados, que indiquem: 1.1. O melhor posicionamento dos dispositivos pontos de acesso de rede sem fio para a maximização da cobertura do sinal de RF; 1.2. A quantidade exata de pontos de acesso a serem instalados por prédio; 1.3. Fontes e zonas de interferência; 1.4. O canal de frequência a ser utilizado por cada ponto de acesso; 1.5. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF em desenho colorido; 2. A unidade de serviço deve contemplar um campus independente da sua localidade; 3. Será de responsabilidade da CONTRATANTE a disponibilização de planta arquitetônica em CAD (*.dwg) para realização de predição teórica e confecção de as-built; 4. Será de responsabilidade da CONTRATADA os seguintes serviços abaixo: 4.1. A disponibilização de um ou mais técnicos para realização de testes em campos para determinar a melhor disposição dos pontos de acesso de rede sem fio; 4.2. Relatório técnico de vistoria resultante da predição teórica das plantas fornecidas pela CONTRATANTE com as seguintes informações: 4.2.1. As possíveis limitações físicas ou dificuldades de implementação detectados nos locais – restrições da construção, obstáculos, etc.; 4.2.2. Melhor posicionamento dos dispositivos em cada andar das localidades visando a maximização da cobertura do sinal de RF; 4.2.3. A quantidade exata de pontos de acesso a ser instalados em cada andar e locais previstos no projeto; 4.2.4. As zonas e faixas de interferência detectadas durante o mapeamento de rádio frequência; 4.2.5. As faixas de frequência a serem utilizadas para cada ponto de acesso; 4.2.6. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF avaliados durante o mapeamento; 5. O relatório técnico deverá ser emitido com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 6. Todos os instrumentos/equipamentos e softwares necessários para a execução do serviço serão fornecidos pela CONTRATADA; 7. O relatório técnico de vistoria com o resultado do estudo de site survey deverá ser entregue ao analista ou técnico de TI lotados no câmpus em avaliação, em via impressa ou em meio digital em até 30 (trinta) dias úteis após assinatura do contrato para os itens acima citados.	SERVIÇO	10	9.245,13	92.451,30
12	SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPOS 1, 2, 3 E 4 --> Características Mínimas: 1. Entende-se por configuração da solução a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CONTRATANTE; 2. O serviço deverá contemplar a configuração de uma unidade da Solução de gerenciamento de redes e segurança para campus tipos 1, 2, 3 ou 4 especificados nesse processo; 3. Deverá contemplar também a adição do(s) dispositivo(s) da solução na ferramenta de gerenciamento centralizado; 4. O	SERVIÇO	10	25.010,10	250.101,00

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	serviço de configuração poderá ser realizado de maneira 100% remota, desde que devidamente acordado e documentado entre a CONTRATANTE e a CONTRATADA; 5. São de responsabilidade da CONTRATADA, entre outras atividades: 5.1. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos firewalls em produção no ambiente atual para a nova solução; 5.2. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões; 5.3. Configurar as funcionalidades relevantes a implementação da solução como: Endereçamento, VLANs, LACP, DHCP e tipos NAT; 5.4. Configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF; 5.5. Realizar a configuração das políticas de firewall analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários e grupos de usuários; 5.6. Implementar políticas de bloqueios de arquivos; 5.7. Configurar limitações de banda com base no IP de origem, usuários e grupos; 5.8. Configurar regras de IPS, Anti-Malware e Filtro URL; 5.9. Configuração da ferramenta de gerenciamento centralizado; 5.10. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório da CONTRATANTE, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação; 5.11. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado; 5.12. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser; 5.13. Configuração das assinaturas de wIDS/Wips; 5.14. Configuração de políticas de bloqueio de rogue APs; 5.15. Configuração para classificação/detecção de interferências WiFi e não-WiFi; 5.16. Configuração dos pontos de acesso sem fio; 5.17. Configuração de SSIDs; 5.18. Configuração do controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança; 5.19. Configuração de um portal de autenticação web para os usuários visitantes, com as seguintes funcionalidades: 5.19.1. Funcionar de forma criptografada com o uso de certificados (SSL); 5.19.2. Customizar com logotipo e políticas de acesso; 5.19.3. Check-box para aceite com as políticas de acesso da rede; 6. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 7. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 8. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 9. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 10. A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE; 11. Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI; 12. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 13. O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia; 14. A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta; 15. Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a “DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO” contendo todas as informações da implantação: 15.1. Aspecto da arquitetura implantada; 15.2. Configuração; 15.3. Descrição das características e recursos utilizados; 15.4. Testes e integração dos ambientes de redes locais da instalação; 16. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 17. A documentação poderá ser entregue em via impressa ou meio digital; 18. A documentação deverá validada pela equipe técnica da CONTRATANTE; 19. Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRADADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE; 20. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formado de repasse de conhecimentos com carga horaria mínima de 8 horas;				
13	SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5 1. Entende-se por configuração da solução a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CONTRATANTE; 2. O serviço deverá contemplar a configuração de uma unidade da Solução de gerenciamento de redes e segurança para campus tipo 5 e a instalação e configuração da ferramenta de	SERVIÇO	1	50.759,57	50.759,57

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	gerenciamento centralizado especificado nesse processo; 3. O serviço de configuração poderá ser realizado de maneira 100% remota, desde que devidamente acordado e documentado entre a CONTRATANTE e a CONTRATADA; 4. São de responsabilidade da CONTRATADA, entre outras atividades: 4.1. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos firewalls em produção no ambiente atual para a nova solução; 4.2. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões; .4.3. Configurar as funcionalidades relevantes a implementação da solução como: Endereçamento, VLANs, LACP, DHCP e tipos NAT; 4.4. Configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF; 4.5. Realizar a configuração das políticas de firewall analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários e grupos de usuários; 4.6. Implementar políticas de bloqueios de arquivos; 4.7. Configurar limitações de banda com base no IP de origem, usuários e grupos; 4.8. Configurar regras de IPS, Anti-Malware e Filtro URL; 4.9. Configuração da ferramenta de gerenciamento centralizado; 4.10. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório da CONTRATANTE, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação; 4.11. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado; 4.12. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser; 4.13. Configuração das assinaturas de wIDS/Wips; 4.14. Configuração de políticas de bloqueio de rogue APs; 4.15. Configuração para classificação/detecção de interferências WiFi e não-WiFi; 4.16. Configuração dos pontos de acesso sem fio; 4.17. Configuração de SSIDs; 4.18. Configuração do controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança; 4.19. Configuração de um portal de autenticação web para os usuários visitantes, com as seguintes funcionalidades: 4.19.1. Funcionar de forma criptografada com o uso de certificados (SSL); 4.19.2. Customizar com logotipo e políticas de acesso; 4.19.3. Check-box para aceite com as políticas de acesso da rede; 5. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 6. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 7. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação; 8. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 9. A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE; 10. Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI; 11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação; 12. O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia; 13. A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta; 14. Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a “DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO” contendo todas as informações da implantação: 14.1. Aspecto da arquitetura implantada; 14.2. Configuração; 14.3. Descrição das características e recursos utilizados; 14.4. Testes e integração dos ambientes de redes locais da instalação; 15. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 16. A documentação poderá ser entregue em via impressa ou meio digital; 17. A documentação deverá validada pela equipe técnica da CONTRATANTE; 18. Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRADADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE; 19. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formado de repasse de conhecimentos com carga horaria mínima de 8 horas;				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
14	INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 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 os pontos de acesso deste processo 3. Deve fornecer no mínimo 30 Watts para alimentação do dispositivo com suporte PoE atendendo ao padrão IEEE 802.3at; 4. Deve acompanhar cabos de energia e acessórios para o seu perfeito funcionamento; 5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática. Deve acompanhar o cabo de alimentação; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).******** Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012.	UNIDADE	270	1.692,00	456.840,00
15	SWITCH TIPO 1 – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 5. Deve possuir 1 (uma) interface USB; 6. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 260 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 32.000 endereços; 9. Deve operar com latência igual ou inferior à 1us (microsegundo); 10. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 11. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente; 12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 13. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos os switches como uma única interface lógica; 14. Deve suportar a comutação de Jumbo Frames; 15. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 16. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 17. Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 18. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos; 19. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 20. Deverá suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 21. Deve implementar serviço de DHCP Server e DHCP Relay; 22. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela; 23. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN); 24. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN; 25. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 26. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 27. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2; 28. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 29. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 30. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 31. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 32. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 33. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 34. Deverá	UNIDADE	6	21.455,75	128.734,50

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 35. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; 36. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ); 37. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 38. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados; 39. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement; 40. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 41. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 42. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 43. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 44. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 45. Deve suportar MAC Authentication Bypass (MAB); 46. Deve implementar RADIUS CoA (Change of Authorization); 47. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 48. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 49. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 50. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 51. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 52. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 53. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 54. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 55. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 56. Deve ser capaz de autorizar a transmissão de pacotes nas interfaces somente para aqueles endereços IP que foram aprendidos dinamicamente através de DHCP Snooping. Os pacotes originados por endereços IP desconhecidos deverão ser descartados; 57. Deve suportar o protocolo PTP (Precision Time Protocol); 58. Deve implementar Netflow, sFlow ou similar; 59. Deve suportar o envio de mensagens de log para servidores externos através de syslog; 60. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 61. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 62. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 63. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 64. Deve permitir ser gerenciado através de IPv6; 65. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 66. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 67. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 68. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 69. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo; 70. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 71. Deverá suportar ser configurado e monitorado através de REST API; 72. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark; 73. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash; 74. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE); 75. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 76. Deve suportar temperatura de operação de até 45º Celsius; 77. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 78. Deve ser fornecido com fontes de alimentação redundantes e internas ao equipamento, com capacidade para operar em tensões de 110V e 220V; 79. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 80. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 81. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 82. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 83. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas,				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
16	PONTO DE ACESSO INDOOR – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio; 21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA; 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 31. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea; 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; 39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique	UNIDADE	250	5.232,23	1.308.057,50

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 42. Deve implementar o padrão IEEE 802.11e; 43. Deve implementar o padrão IEEE 802.11h; 44. Deve implementar o padrão IEEE 802.3az; 45. Deve suportar ser gerenciado via SNMP; 46. Deve suportar consultas via REST API; 47. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação; 48. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C; 49. Deve suportar sistema antifurto do tipo Kensington Security Lock ou similar; 50. Deve possuir indicadores luminosos (LED) para indicação de status; 51. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 52. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 53. Deve possuir certificado emitido pela Wi-Fi Alliance; 54. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 55. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
17	PONTO DE ACESSO OUTDOOR - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN; 11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 13. Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento; 14. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 18. Deve permitir operação em modo Mesh; 19. Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz; 20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio; 21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 22. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL); 23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 24. Deve implementar recurso de Target Wake Time (TWT) configurado por SSID; 25. Deve suportar BSS Coloring; 26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 27. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20); 28. Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz; 29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 31. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não	UNIDADE	20	10.518,86	210.377,20

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	autorizados, também conhecidos como Rogue Aps; 32. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea; 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X; 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 39. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 40. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 41. Deve implementar o padrão IEEE 802.11e; 42. Deve implementar o padrão IEEE 802.11h; 43. Deve implementar o padrão IEEE 802.3az; 44. Deve suportar consultas SNMP diretamente no ponto de acesso; 45. Deve suportar consultas REST API diretamente no ponto de acesso; 46. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes; 47. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60º C; 48. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção; 49. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios Wi-Fi; 50. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 51. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 52. Deve possuir certificado emitido pela Wi-Fi Alliance; 53. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 54. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
18	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 1---> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 5 (cinco) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 288 (duzentos e oitenta e oito) portas de switch ou um total de 6 (seis) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A	UNIDADE	2	8.685,49	17.370,98

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 8 (oito) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 1.6 Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 300 (trezentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 800 (oitocentos) Mbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 4.2 Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 400.000 (quatrocentas mil) de sessões simultâneas/concorrentes e 28.000 (vinte e oito mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
19	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 2 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 8 (oito) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX;; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 672 (seiscentos e setenta e duas) portas de switch ou um total de 14 (quatorze) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve,	UNIDADE	12	12.969,69	155.636,28

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 30 (trinta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 1.6 Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 600 (seiscentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 1.5 Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução dev erá ser capaz de tratar 6.2 Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 600.000 (seiscentas mil) de sessões simultâneas/concorrentes e 30.000 (trinta mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
20	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 3 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 10 (dez) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 672 (seiscentos e setenta e duas) portas de switch ou um total de 14 (quatorze) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos	UNIDADE	6	21.988,40	131.930,40

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 40 (quarenta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 3.2 Gbps de tráfego encapsulado via VPN; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 3.74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 700 (setecentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 1.5 Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 9 (nove) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 1.400.000 (um milhão e quatrocentas mil) de sessões simultâneas/concorrentes e 40.000 (quarenta mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
21	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 4 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 2 (duas) interfaces 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede; 4. Cada appliance físico deve possuir fontes de alimentações redundantes com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar os cabos de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados	UNIDADE	6	54.375,89	326.255,34

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 1440 (um mil, quatrocentas e quarenta) portas de switch ou um total de 30 (trinta) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 60 (sessenta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A solução deverá ser capaz de encaminhar 3.2 Gbps de tráfego encapsulado via VPN; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 900 (novecentos) Mbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 2 (dois) Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	tratar 16 (dezesseis) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 1.400.000 (um milhão e quatrocentas mil) de sessões simultâneas/concorrentes e 50.000 (cinquenta mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
22	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 4 (quatro) interfaces 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X ou superior para permitir a conexão com a rede; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste	UNIDADE	1	156.389,16	156.389,16

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 3360 (três mil, trezentos e sessenta) portas de switch ou um total de 70 (setenta) switches; 13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados; 15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 500 (quinhentos) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 36. A A solução deverá ser capaz de encaminhar 9 (nove) Gbps de tráfego encapsulado via VPN IPSec; 37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 42. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 47. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 48. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 49. A solução deve permitir o				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: 74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); 74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; 74.3. ASLEAP; 74.4. Null Probe Response or Null SSID Probe Response; 74.5. Long Duration; 74.6. Ataques contra Wireless Bridges; 74.7. Weak WEP; 74.8. Invalid MAC OUI. 75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 81. Quando usando				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 84. A solução deverá suportar Single-Sign-On (SSO); 85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 91. A solução deve permitir a configuração do captive portal com endereço IPv6; 92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 99. A solução deverá ser capaz de inspecionar 4.5 Gbps de tráfego SSL; 100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar; 103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 113. A solução deverá ser capaz de tratar 14 (quatorze) Gbps de tráfego por meio do filtro de aplicações; 114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 117. A solução deverá permitir a criação manual de novos padrões de aplicações; 118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	IPv6), portas e protocolos; 123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 126. A solução deverá ser capaz de tratar 35 (trinta e cinco) Gbps de tráfego por meio das regras de firewall stateful; 127. A solução deverá ser capaz de suportar 7.000.000 (sete milhões) de sessões simultâneas/concorrentes e 400.000 (quatrocentas mil) novas sessões por segundo; 128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 130. A solução deverá suportar PBR – Policy Based Routing; 131. A solução deverá suportar roteamento multicast; 132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 133. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 152. A solução deverá suportar Netflow ou sFlow; 153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
				Valor Total do Lote/Grupo: R$ 4.313.772,68	

Valor Total do Processo: R$ 4.746.341,68

SIPAC | DTIC - Diretoria de Tecnologia da Informação e Comunicação - (48) 3877-9000 | Copyright © 2005-2021 - UFRN - appdocker1-srv1.appdocker1-inst1